



Notes de mise à jour de Cisco Secure Firewall Threat Defense, version 7.2.x

Dernière modification : 2026-05-22

Notes de mises à niveau de Cisco Secure Firewall Threat Defense

Ce document contient des informations sur la version de :

- Propriété Cisco Secure Firewall Threat Defense
- Cisco Cisco Secure Firewall Management Center (sur site)
- Propriété Cisco Secure Firewall device manager

Pour les déploiements dans le cloud, consultez le [Notes de mise à jour de Cisco Firewall Management Center en nuage](#) ou [Nouveautés pour Security Cloud Control](#).

Dates de publication

Tableau 1 : Dates de la version 7.2

Version	Créer	Date	Plateformes
7.2.10.2	2	25/09/2025	Tous
7.2.10.1	10	2025-09-4	On-Prem Firewall Management Center
7.2.10	210	2025-05-22	Tous les types de documents
7.2.9	44	2024-10-22	Tous les types de documents
7.2.8.1	17	2024-08-26	Tous les types de documents
7.2.8	25	2024-06-24	Tous les types de documents
7.2.7	500	2024-04-29	Tous les types de documents
7.2.6	168	2024-04-22	N'est plus disponible.
	167	2024-03-19	N'est plus disponible.
7.2.5.2	4	2024-05-06	Tous les types de documents
7.2.5.1	29	2023-11-14	Tous les types de documents
7.2.5	208	2023-07-27	Tous les types de documents
7.2.4.1	43	2023-07-27	Tous les types de documents

Version	Créer	Date	Plateformes
7.2.4	169	10-05-2023	On-Prem Firewall Management Center
	165	2023-05-03	Appareils
7.2.3.1	13	2023-04-18	On-Prem Firewall Management Center
7.2.3	77	2023-02-27	Tous les types de documents
7.2.2	54	2022-11-29	Tous les types de documents
7.2.1	40	2022-10-03	Tous les types de documents
7.2.0.1	12	2022-08-10	Tous les types de documents
7.2.0	82	2022-06-06	Tous les types de documents

Compatibilité

Avant d’effectuer une mise à niveau ou une recréation d’image, assurez-vous que la version cible est compatible avec votre déploiement. Si vous ne pouvez pas procéder à une mise à niveau ou à une recréation d’image en raison d’une incompatibilité, contactez votre représentant Cisco ou la personne-ressource du partenaire pour obtenir des renseignements.

Pour des renseignements sur la compatibilité, consultez :

- [Guide de compatibilité de Cisco Secure Firewall Management Center](#)
- [Guide de compatibilité de Cisco Secure Firewall Threat Defense](#)
- [Compatibilité FXOS de Cisco Firepower 4100/9300](#)

Fonctionnalités

Pour les fonctionnalités des versions antérieures, consultez [Nouvelles fonctionnalités de Cisco Secure Firewall Management Center par version](#) et [Nouvelles fonctionnalités de Cisco Secure Firewall Device Manager par version](#).

Incidence sur la mise à niveau

Une fonctionnalité a une incidence sur la mise à niveau si sa mise à niveau et son déploiement peuvent forcer le système à traiter le trafic ou à agir différemment sans autre action de votre part. Cela arrive fréquemment avec les nouvelles capacités de détection des menaces et d’identification des applications. Une fonctionnalité peut également avoir une incidence sur la mise à niveau si celle-ci implique que vous preniez des mesures avant ou après la mise à niveau pour éviter un résultat indésirable; par exemple, si vous devez modifier une configuration.

Les descriptions des fonctionnalités comprennent, le cas échéant, l’incidence de la mise à niveau. Pour obtenir une liste plus complète des fonctionnalités ayant une incidence sur les mises à niveau par version, consultez [Fonctionnalités et incidence de la mise à niveau, à la page 46](#).

Fonctionnalités des versions de maintenance

Les fonctionnalités, les améliorations et les correctifs critiques inclus dans les versions de maintenance (troisième chiffre) et les correctifs (quatrième chiffre) peuvent ignorer les versions futures, selon la date de version, le type de version (court ou long terme) et d'autres facteurs. Minimisez l'incidence de la mise à niveau et autres en accédant directement à la dernière version de maintenance de la version choisie. Voir [Choix de votre cible de mise à niveau, à la page 51](#).

Si vous utilisez l'interface Web dans une langue autre que l'anglais, les fonctionnalités introduites dans les versions de maintenance et les correctifs peuvent ne pas être traduites avant la prochaine version majeure.

Fonctionnalités de Snort

Snort 3 est la plateforme d'inspection par défaut pour Firewall Threat Defense. Les fonctionnalités de Snort 3 pour les déploiements On-Prem Firewall Management Center s'appliquent également à Firepower Device Manager, même si elles ne sont pas répertoriées en tant que nouvelles fonctionnalités Firepower Device Manager. Cependant, gardez à l'esprit que On-Prem Firewall Management Center peut offrir des options plus configurables que Firepower Device Manager.



Important Snort 2 est obsolète dans la version 7.7 et les versions ultérieures, et empêche la mise à niveau de Firewall Threat Defense. Si vous utilisez toujours Snort 2 sur d'anciens périphériques, passez à Snort 3 pour améliorer la détection et les performances.

Règles de prévention des intrusions et mots clés

Les mises à niveau peuvent importer et activer automatiquement des règles de prévention des intrusions et de préprocesseurs nouvelles et mises à jour, les états modifiés pour les règles existantes et les paramètres de politique de prévention des intrusions par défaut modifiés. Si une nouvelle règle de prévention des intrusions utilise des mots clés qui ne sont pas pris en charge dans votre version actuelle, cette règle n'est pas importée lorsque vous mettez à jour SRU ou LSP. Après la mise à niveau et la prise en charge de ces mots clés, les nouvelles règles de prévention des inclusions sont importées et, selon la configuration IPS, peuvent être activées automatiquement et commencer à générer des événements et à affecter le flux de trafic.

Pour plus de renseignements sur les nouveaux mots clés, consultez les notes de mise à jour de Snort: <https://www.snort.org/downloads>.

FlexConfig

Les mises à niveau peuvent ajouter une interface Web ou la prise en charge de Smart CLI pour des fonctionnalités qui nécessitent déjà FlexConfig. Bien que vous ne puissiez pas affecter ou créer des objets FlexConfig à l'aide de commandes obsolètes, dans la plupart des cas, les FlexConfig existantes continuent de fonctionner et vous pouvez toujours les déployer. Cependant, l'utilisation de commandes obsolètes peut parfois entraîner des problèmes de déploiement. La mise à niveau ne convertit pas les FlexConfigs. Après la mise à niveau, configurez les nouvelles fonctionnalités prises en charge dans l'interface Web ou Smart CLI. Lorsque vous êtes satisfait de la nouvelle configuration, supprimez les FlexConfigs obsolètes.

Les descriptions de fonctionnalités incluent des informations sur les FlexConfigs obsolètes, le cas échéant. Pour obtenir la liste complète des FlexConfigs obsolètes, consultez votre guide de configuration.

Intégrations et journalisation

Ces intégrations et fonctions de journalisation peuvent comporter de nouvelles fonctionnalités associées aux versions de Threat Defense et du Management Center :

- Syslog : [Messages Syslog de Cisco Secure Firewall Threat Defense](#)
- Cisco Success Network : [Données de télémétrie de Cisco Success Network collectées à partir de Cisco Secure Firewall Management Center](#)
- API REST : [Guide de démarrage rapide de Cisco Secure Firewall Management Center REST API](#) et [Guide de Cisco Secure Firewall Threat Defense REST API](#)

On-Prem Firewall Management Center Fonctionnalités de la version 7.2.10

Tableau 2 : On-Prem Firewall Management Center Fonctionnalités de la version 7.2.10

Caractéristiques	Version Management Center	Défense Version minimale de Threat Defense	Détails
Fonctionnalités des versions de maintenance antérieures			
Fonctionnalités des versions de maintenance antérieures.	Dépend de la fonctionnalité	Dépend de la fonctionnalité	La version 7.2.10 comporte également : • Incidence sur la mise à niveau Nouvelle méthode de connexion en nuage Cisco Advanced Malware Protection. (7.0.7) • Sauvegardes de connexions au nuage Cisco Advanced Malware Protection obsolètes. (7.0.7) • Incidence sur la mise à niveau Exiger l'attribut Message-Authenticator dans toutes les réponses RADIUS. (7.0.7) • Incidence sur la mise à niveau Mise à jour des exigences d'accès Internet pour les licences Smart. (7.0.8)
Mise à jour			
Firewall Threat Defense et assistants de mise à niveau de châssis optimisés pour les écrans à faible résolution.	7.2.10 7.6.0	N'importe lequel	Nous avons optimisé les assistants de mise à niveau de châssis et Firewall Threat Defense pour les écrans à faible résolution (et les fenêtres de navigateur plus petites). Le texte semble plus petit et certains éléments de l'écran sont masqués. Si vous changez de résolution ou de taille de fenêtre en cours de session, vous devrez peut-être actualiser la page pour que l'interface Web s'adapte. Notez que la résolution d'écran minimale à utiliser dans le On-Prem Firewall Management Center est de 1280 x 720. Écrans nouveaux ou modifiés : • Devices (périphériques) > Threat Defense Upgrade (mettre à niveau Threat Defense) • Périphériques > Mise à niveau du châssis

Caractéristiques	Version Management Center	Défense Version minimale de Threat Defense	Détails
Rendement			
Le trafic d'applications chiffré à bande passante élevée contourne l'inspection d'intrusion inutile.	7.2.10 7.6.1 7.7.0	7.2.10 avec Snort 3 7.6.1 avec Snort 3 7.7.0	Le trafic d'applications chiffrés à bande passante élevée contourne désormais l'inspection d'intrusion inutile, même si la connexion correspond à une règle Allow (Autoriser). Les mises à jour des règles d'intrusion (LSP) et de la base de données des vulnérabilités (VDB) peuvent modifier la liste des applications exemptées, mais celles actuellement concernées sont : AnyConnect, IPsec, iCloud Private Relay, QUIC (y compris HTTP/3), Webex Media et Secure RTCP.

On-Prem Firewall Management Center Fonctionnalités de FMC dans la version 7.2.9

Tableau 3 : On-Prem Firewall Management Center Fonctionnalités de FMC dans la version 7.2.9

Caractéristiques	FMC minimal	Version Cisco FTD minimale	Détails
Fonctionnalités des versions de maintenance antérieures			
Fonctionnalités des versions de maintenance antérieures.	Dépend de la fonctionnalité	Dépend de la fonctionnalité	La version 7.2.9 comporte également : • Régions Plateforme Cisco Security Cloud : Inde et Australie. (7.0.7)
Nuage public et privé			
Prise en charge de VMware vSphere/VMware ESXi 8.0.	7.2.9 7.4.2 7.6.0	7.2.9 7.4.2 7.6.0	Vous pouvez maintenant déployer Cisco Secure Firewall Threat Defense Virtual et Firewall Management Center Virtual sur VMware vSphere/VMware ESXi 8.0. Voir : Guide de démarrage de Cisco Secure Firewall Threat Defense Virtual
Contrôle d'accès : détection des menaces et identification des applications			
Gestion du trafic asymétrique.	7.2.9 7.4.2 7.6.0	7.2.9 avec Snort 3 7.4.2 avec Snort 3 7.6.0 avec Snort 3	Incidence sur la mise à niveau. Les connexions éligibles sont désormais inspectées et gérées. Dans les déploiements à routage asymétrique, le dispositif de Firewall Threat Defense inspecte désormais le côté de la connexion qu'il peut observer. Aucune configuration supplémentaire n'est requise.

Fonctionnalités de On-Prem Firewall Management Center dans la version 7.2.8

Tableau 4 : Fonctionnalités de On-Prem Firewall Management Center dans la version 7.2.8

Caractéristiques	Version minimale Management Center	Défense Version minimale de Threat Defense	Détails
Plateforme			
Firewall Threat Defense Virtual pour Metaport.	7.2.8 7.3.0	7.2.8 7.3.0	Nous avons introduit Firewall Threat Defense Virtual pour Megaport (Megaport Virtual Edge). La haute disponibilité est prise en charge. La mise en grappe n'est pas prise en charge. Restrictions de version : au départ, vous ne pourrez peut-être pas déployer les versions 7.3.x ou 7.4.x. Déployez plutôt les versions 7.2.8–7.2.x et effectuez la mise à niveau. Voir : Guide de démarrage de Cisco Secure Firewall Threat Defense Virtual

On-Prem Firewall Management Center Nouvelles fonctionnalités dans la version 7.2.7

Cette version présente des améliorations en matière de stabilité, de renforcement et de performances. Consultez [Bogues résolus dans la version 7.2.7](#), à la page 95.

Fonctionnalités On-Prem Firewall Management Center de la version 7.2.6

Suite au bogue [CSCwi63113](#), la version 7.2.6 a été reportée le 29-04-2024 et n'est plus téléchargeable. Si vous l'avez téléchargée, ne l'utilisez pas. Si vous utilisez cette version, effectuez la mise à niveau. Les fonctionnalités répertoriées ici sont également disponibles dans la version 7.2.7.

Tableau 5 : Fonctionnalités On-Prem Firewall Management Center de la version 7.2.6

Caractéristiques	Version Management Center	Défense Version minimale de Threat Defense	Détails
Fonctionnalités des versions de maintenance antérieures			
Fonctionnalités des versions de maintenance antérieures.	Dépend de la fonctionnalité	Dépend de la fonctionnalité	La version 7.2.6 comporte également : Incidence sur la mise à niveau Mise à jour du fournisseur de services d'analyse web. (7.0.6)
Interfaces			

Caractéristiques	Version Management Center	Défense Version minimale de Threat Defense	Détails
Configurez les interfaces de confiance de relais DHCP à partir de l'interface Web du On-Prem Firewall Management Center.	7.2.6 7.4.1	N'importe lequel	Incidence sur la mise à niveau. Répétez toutes les configurations FlexConfig connexes après la mise à niveau. Vous pouvez désormais utiliser l'interface Web du On-Prem Firewall Management Center pour configurer des interfaces en tant qu'interfaces de confiance afin de conserver l'option 82 de DHCP. Ce faisant, ces paramètres remplacent toutes les configurations FlexConfig existantes, bien que vous deviez les supprimer. L'option 82 DHCP est utilisée par les commutateurs et les routeurs en aval pour la surveillance DHCP et la protection source IP. Normalement, si l'agent de relais DHCP Firewall Threat Defense reçoit un paquet DHCP avec l'option 82 déjà définie, mais que le champ giaddr (qui spécifie l'adresse de l'agent de relais DHCP définie par le dernier avant de transmettre le paquet au serveur) est réglé sur 0, puis Firewall Threat Defense supprimera ce paquet par défaut. Vous pouvez conserver l'option 82 et transférer le paquet en identifiant une interface comme interface de confiance. Écrans nouveaux ou modifiés : Périphériques > Gestion des périphériques > Ajouter/modifier un périphérique > DHCP > Relais DHCP Consultez : Configurer les agents de relais DHCP.
NAT			
Créer des groupes de réseaux lors de la modification des règles NAT.	7.2.6 7.4.1	N'importe lequel	Vous pouvez désormais créer des groupes de réseaux en plus des objets réseau lors de la modification d'une règle NAT. Consultez : Personnalisation des règles NAT pour plusieurs périphériques.
Haute disponibilité/évolutivité : Threat Defense			
Réduction du nombre de « faux basculements » pour une haute disponibilité de Firewall Threat Defense.	7.2.6 7.4.0	7.2.6 7.4.0	Voir : Redondance du module heartbeat
Haute disponibilité : Management Center			
Fichier de sauvegarde unique pour les On-Prem Firewall Management Center à haute disponibilité.	7.2.6 7.4.1	N'importe lequel	Lors d'une sauvegarde de configuration uniquement du On-Prem Firewall Management Center active dans une paire à haute disponibilité, le système crée désormais un fichier de sauvegarde unique que vous pouvez utiliser pour restaurer l'une ou l'autre des unités. Consultez : Sauvegarde unifiée des centres de gestion en haute disponibilité
Journalisation et analyse des événements			

Caractéristiques	Version Management Center	Défense Version minimale de Threat Defense	Détails
Ouvrir le traceur de paquets à partir de la visionneuse d'événements unifiés.	7.2.6 7.4.1	N'importe lequel	Vous pouvez maintenant ouvrir Packet Tracer à partir de la vue unifiée des événements (Analysis > Unified Events). Cliquez sur l'icône de points de suspension (...) à côté de l'événement souhaité et cliquez sur Open in Packet Tracer (Ouvrir dans le traceur de paquets). Restrictions de versions : dans la version 7.2.x, utilisez l'icône de développement (>) au lieu de l'icône de points de suspension. Consultez : Travailler avec la visionneuse d'événements unifiée

surveillance de l'intégrité

Alertes d'intégrité pour un espace disque excessif utilisé par les fichiers d'historique de déploiement (restauration).	7.2.6 7.4.1	N'importe lequel	Le module d'analyse de l'intégrité du disque signale désormais si les fichiers d'historique de déploiement (restauration) utilisent un espace disque excessif sur le On-Prem Firewall Management Center. Déployer la politique d'intégrité du On-Prem Firewall Management Center après la mise à niveau. Voir : Alerte sur l'intégrité du disque pour les fichiers historiques de configuration du périphérique
Alertes d'intégrité pour les problèmes de synchronisation NTP.	7.2.6 7.4.1	N'importe lequel	Un nouveau module d'intégrité d'état du serveur d'horloge signale les problèmes de synchronisation NTP. Déployer la politique d'intégrité du On-Prem Firewall Management Center après la mise à niveau. Voir : Synchronisation de l'heure et modules d'intégrité

Déploiement et gestion des politiques

Afficher et générer des rapports sur les modifications de configuration depuis votre dernier déploiement.	7.2.6 7.4.1	N'importe lequel	Vous pouvez générer, afficher et télécharger les rapports suivants sous forme de fichier compressé sur les modifications de configuration depuis votre dernier déploiement : • Un rapport sur les <i>modifications de politique</i> pour chaque périphérique qui présente un aperçu des ajouts, des modifications ou des suppressions dans la politique ou des objets qui doivent être déployés sur le périphérique. • Un <i>rapport consolidé</i> qui classe chaque périphérique en fonction de l'état de la génération de rapport sur les modifications de politique. Cela est particulièrement utile après la mise à niveau du On-Prem Firewall Management Center ou des Firewall Threat Defenses, afin que vous puissiez voir les modifications apportées par la mise à niveau avant de procéder au déploiement. Écrans nouveaux ou modifiés : Deploy > Advanced Deploy (Déployer > Déploiement avancé). Consultez : Télécharger le rapport sur les modifications de politiques pour plusieurs périphériques.
---	----------------	------------------	---

Caractéristiques	Version Management Center	Défense Version minimale de Threat Defense	Détails
Définissez le nombre de fichiers d'historique de déploiement à conserver pour la restauration du périphérique.	7.2.6 7.4.1	N'importe lequel	Vous pouvez désormais définir le nombre de fichiers d'historique de déploiement à conserver pour la restauration du périphérique, jusqu'à dix (valeur par défaut). Cela peut vous aider à économiser de l'espace disque sur le On-Prem Firewall Management Center. Écrans nouveaux ou modifiés : Deploy (Déployer) > Deployment History (Historique des déploiements) > Deployment Setting (Paramètres de déploiement) > Configuration Version Setting (Paramètre de version de configuration) Consultez : Définir le nombre de versions de configuration.
Mise à jour			

Caractéristiques	Version Management Center	Défense Version minimale de Threat Defense	Détails
Amélioration de la page de démarrage de la mise à niveau et de la gestion des paquets.	7.2.6 7.4.1	N'importe lequel	

Caractéristiques	Version Management Center	Défense Version minimale de Threat Defense	Détails
			Une nouvelle page de mise à niveau facilite le choix, le téléchargement, la gestion et l'application des mises à niveau à l'ensemble de votre déploiement. Cela concerne le On-Prem Firewall Management Center, les Firewall Threat Defense et tout ancien périphérique NGIPSv/ASA FirePOWER. La page répertorie tous les paquets de mise à niveau qui s'appliquent à votre déploiement actuel, avec des versions suggérées spécialement indiquées. Vous pouvez facilement choisir et télécharger directement des paquets de Cisco, ainsi que téléverser et supprimer manuellement des paquets. Un accès Internet est nécessaire pour récupérer la liste et télécharger directement des paquets de mise à niveau. Sinon, vous êtes limité à une gestion manuelle. Les correctifs ne sont pas répertoriés, sauf si vous avez au moins un périphérique à la version de maintenance appropriée (ou si vous avez téléchargé le correctif manuellement). Vous devez téléverser manuellement les correctifs. Écrans nouveaux ou modifiés : • System (Système)( > Product Upgrades (Mises à niveaux des produits) est désormais l'endroit où vous mettez à niveau le On-Prem Firewall Management Center et tous les périphériques gérés, ainsi que la gestion des logiciels de mise à niveau. • System (système)( > Content Updates (mises à jour de contenu) vous permettent désormais de mettre à jour les règles de prévention des intrusions, la VDB et la GeoDB. • Devices (Périphériques) > Threat Defense Upgrade (Mise à niveau de la défense contre les menaces) vous permet d'accéder directement à l'assistant de mise à niveau de la Firewall Threat Defense. • System (système)( > Users (utilisateurs) > User Role (rôle d'utilisateur) > Create User Role (créer un rôle d'utilisateur) > Menu-Based Permissions (autorisations basées sur le menu) vous permettent désormais d'accorder l'accès aux Content Updates (mises à jour de contenu) (VDB, GeoDB, règles de prévention des intrusions) sans permettre l'accès aux Product Upgrades (mises à niveau de produits) (logiciel du système). Écrans ou options obsolètes : • System (système)( > Updates (mises à jour) sont obsolètes. Toutes les mises à niveau de la Firewall Threat Defense utilisent désormais l'assistant. • Le bouton Add Upgrade Package (Ajouter un paquet de mise à niveau) de l'assistant de mise à niveau de Firewall Threat Defense a été remplacé par un lien Manage Upgrade Packages (Gérer les paquets de mise à niveau) vers la nouvelle page de mise à niveau.

Caractéristiques	Version Management Center	Défense Version minimale de Threat Defense	Détails
			Voir : Guide pour le centre de gestion de Cisco Secure Firewall Threat Defense Upgrade
Activer le retour arrière à partir de l'assistant de mise à niveau de Firewall Threat Defense.	7.2.6 7.4.1	N'importe lequel, en cas de mise à niveau vers la version 7.1 ou ultérieure	Vous pouvez maintenant activer le retour arrière à partir de l'assistant de mise à niveau de Firewall Threat Defense. Autres restrictions de version : vous devez mettre à niveau Firewall Threat Defense vers la version 7.1. Non pris en charge avec le On-Prem Firewall Management Center version 7.3.x ou 7.4.0. Voir : Guide pour le centre de gestion de Cisco Secure Firewall Threat Defense Upgrade
Sélectionner les périphériques à mettre à niveau dans l'assistant de mise à niveau de Firewall Threat Defense.	7.2.6 7.3.0	N'importe lequel	Utilisez l'assistant pour sélectionner les périphériques à mettre à niveau. Vous pouvez désormais utiliser l'assistant de mise à niveau de Firewall Threat Defense pour sélectionner ou affiner les périphériques à mettre à niveau. Dans l'assistant, vous pouvez basculer l'affichage entre les périphériques sélectionnés, les candidats à la mise à niveau restants, les périphériques non admissibles (avec les motifs), les périphériques qui ont besoin du paquet de mise à niveau, etc. Auparavant, vous ne pouviez utiliser que la page de gestion des périphériques et le processus était beaucoup moins flexible. Voir : Guide pour le centre de gestion de Cisco Secure Firewall Threat Defense Upgrade
Afficher l'état de mise à niveau détaillé à partir de l'assistant de mise à niveau de Firewall Threat Defense.	7.2.6 7.4.1	N'importe lequel	La dernière page de l'assistant de mise à niveau de Firewall Threat Defense vous permet désormais de surveiller la progression de la mise à niveau. Cela s'ajoute à la capacité de surveillance existante sous l'onglet Mise à niveau sur la page de gestion des périphériques et sur le centre de messages. Notez que tant que vous n'avez pas commencé un nouveau flux de mise à niveau, la mise à niveau des périphériques > Threat Defense vous ramène à cette dernière page de l'assistant, où vous pouvez afficher l'état détaillé de la mise à niveau du périphérique en cours (ou la plus récente). Voir : Guide pour le centre de gestion de Cisco Secure Firewall Threat Defense Upgrade
Mises à niveau de la Firewall Threat Defensesans surveillance.	7.2.6 7.3.0	N'importe lequel	L'assistant de mise à niveau Firewall Threat Defense prend désormais en charge les mises à niveau sans surveillance, à l'aide d'un nouveau menu Unattended Mode (mode sans surveillance). Il vous suffit de sélectionner la version cible et les périphériques que vous souhaitez mettre à niveau, de spécifier quelques options de mise à niveau et de partir. Vous pouvez même vous déconnecter ou fermer le navigateur. Voir : Guide pour le centre de gestion de Cisco Secure Firewall Threat Defense Upgrade

Caractéristiques	Version Management Center	Défense Version minimale de Threat Defense	Détails
Flux de mise à niveau simultanée de Firewall Threat Defense par différents utilisateurs.	7.2.6 7.3.0	N'importe lequel	Nous autorisons désormais les flux de travail de mise à niveau simultanée par différents utilisateurs, pourvu que vous mettez à niveau différents périphériques. Le système vous empêche de mettre à niveau des périphériques déjà présents dans le flux de travail d'une autre personne. Auparavant, un seul flux de travail de mise à niveau était autorisé à la fois pour tous les utilisateurs. Voir : Guide pour le centre de gestion de Cisco Secure Firewall Threat Defense Upgrade
Ignorez la génération de dépannage avant la mise à niveau pour les périphériques de Firewall Threat Defense.	7.2.6 7.3.0	N'importe lequel	Vous pouvez désormais ignorer la génération automatique des fichiers de dépannage avant les mises à niveau majeures et de maintenance en désactivant la nouvelle option Generate troubleshooting files before upgrade begins (Générer les fichiers de dépannage avant le début de la mise à niveau). Cela permet de gagner du temps et de l'espace disque. Pour générer manuellement des fichiers de dépannage pour un périphérique Firewall Threat Defense, choisissez System (système)(⚙️) > Health (intégrité) > Monitor (moniteur), cliquez sur le périphérique dans le panneau de gauche, sur View System & Troubleshoot Details (afficher les détails du système et du dépannage), puis sur Generate Troubleshooting Files (générer les fichiers de résolution de problèmes). Voir : Guide pour le centre de gestion de Cisco Secure Firewall Threat Defense Upgrade
Notifications de version suggérée.	7.2.6 7.4.1	N'importe lequel	Le On-Prem Firewall Management Center vous informe désormais lorsqu'une nouvelle version suggérée est disponible. Si vous ne souhaitez pas effectuer la mise à niveau tout de suite, vous pouvez demander au système de vous le rappeler ultérieurement, ou différer les rappels jusqu'à la prochaine version suggérée. La nouvelle page de mise à niveau indique également les versions suggérées. Voir : Nouvelles fonctionnalités de Cisco Secure Firewall Management Center par version
Nouvel assistant de mise à niveau pour le On-Prem Firewall Management Center.	7.2.6 7.4.1	N'importe lequel	Une nouvelle page de démarrage et un nouvel assistant de mise à niveau facilitent la mise à niveau du On-Prem Firewall Management Center. Après avoir utilisé System (Système)(⚙️) > Product Upgrades (Mises à niveau des produits) pour obtenir le paquet de mise à niveau approprié sur le On-Prem Firewall Management Center, cliquez sur Upgrade (Mettre à niveau) pour commencer. Restrictions de version : uniquement pris en charge pour les mises à niveau du On-Prem Firewall Management Center à partir de la version 7.4.1 et ultérieures. Non pris en charge pour les mises à niveau à partir de la version 7.3.x ou 7.4.0. Voir : Guide pour le centre de gestion de Cisco Secure Firewall Threat Defense Upgrade

Caractéristiques	Version Management Center	Défense Version minimale de Threat Defense	Détails
Correctif rapide pour les On-Prem Firewall Management Center à haute disponibilité sans suspendre la synchronisation.	7.2.6 7.4.1	N'importe lequel	Sauf indication contraire dans les notes de version du correctif ou dans le TAC de Cisco, vous n'avez pas besoin d'interrompre la synchronisation pour installer un correctif sur les On-Prem Firewall Management Center à haute disponibilité. Voir : Guide pour le centre de gestion de Cisco Secure Firewall Threat Defense Upgrade

Administration

Mise à jour des exigences d'accès Internet pour le téléchargement direct des mises à niveau logicielles.	7.2.6 7.4.1	N'importe lequel	Incidence sur la mise à niveau. Le système se connecte à de nouvelles ressources. Le On-Prem Firewall Management Center a modifié son emplacement de téléchargement direct pour les paquets de mise à niveau logicielle de sourcefire.com à amazonaws.com. Voir: Sécurité, accès à Internet et ports de communication
--	----------------	------------------	--

Convivialité, performances et dépannage

Activer/désactiver l'optimisation des objets de contrôle d'accès.	7.2.6 7.4.1	N'importe lequel	Vous pouvez maintenant activer et désactiver l'optimisation des objets de contrôle d'accès à partir de l'interface Web du On-Prem Firewall Management Center. Écrans nouveaux ou modifiés : System (Système)( > Configuration > Access Control Preferences (Préférences du contrôle d'accès) > Object Optimization (Optimisation des objets) Autres restrictions de version : l'optimisation des objets de contrôle d'accès est automatiquement activée sur tous les centres de gestion mis à niveau ou recréés vers les versions 7.2.4 à 7.2.5 et 7.4.0, et automatiquement désactivée sur tous les On-Prem Firewall Management Center mis à niveau ou recréés vers la version 7.3.x On-Prem Firewall Management Center. Elle est configurable et activée par défaut pour les On-Prem Firewall Management Center dont l'image a été recrée en version 7.2.6 et ultérieures /7.4.1 et ultérieures, mais respecte votre paramètre actuel lorsque vous passez à ces versions. Consultez : Préférences liées au contrôle d'accès et
---	----------------	------------------	--

Caractéristiques	Version Management Center	Défense Version minimale de Threat Defense	Détails
Outil de ping de liaison de commande de grappe.	7.2.6 7.4.1	N'importe lequel	Vous pouvez vérifier que tous les nœuds de la grappe peuvent communiquer entre eux sur la liaison de commande de grappe en effectuant un ping. L'une des principales causes de l'échec d'un nœud à rejoindre la grappe est une configuration incorrecte de la liaison de commande de la grappe; par exemple, la MTU de la liaison de commande de la grappe peut être plus élevée que les MTU des commutateurs de connexion. Écrans nouveaux ou modifiés : Devices (Périphériques) > Device Management (Gestion des périphériques) > More (Plus) > Cluster Live Status (État en direct de la grappe). Voir : Effectuer un ping sur la liaison de commande de grappe
Snort 3 redémarre lorsqu'il utilise trop de mémoire, ce qui peut déclencher le basculement à haute disponibilité.	7.2.6 7.4.1	7.2.6 avec Snort 3 7.4.1 avec Snort 3	Pour améliorer la continuité des opérations, une utilisation excessive de la mémoire par lSnort peut désormais déclencher un basculement à haute disponibilité. Cela se produit parce que Snort 3 redémarre si le processus utilise trop de mémoire. Le redémarrage du processus Snort interrompt brièvement le flux de trafic et l'inspection sur le périphérique. Ce qui, dans les déploiements à haute disponibilité, peut déclencher le basculement. (Dans un déploiement autonome, les configurations d'interface déterminent si le trafic est interrompu ou s'il passe sans inspection pendant l'interruption). Cette fonction est activée par défaut. Vous pouvez utiliser l'interface de ligne de commande pour le désactiver ou configurer le seuil de mémoire. Restrictions de plateforme : non pris en charge avec les périphériques en grappe. Commandes CLI nouvelles ou modifiées : configure snort3 memory-monitor, show snort3 memory-monitor-status Voir : Référence des commandes de défense contre les menaces de Cisco Secure Firewall
Définir la fréquence des vidages de mémoire de Snort 3.	7.2.6 7.4.1	7.2.6 avec Snort 3 7.4.1 avec Snort 3	Vous pouvez maintenant définir la fréquence des vidages de mémoire de Snort 3. Au lieu de générer un vidage de la mémoire à chaque plantage Snort, vous pouvez en générer un lors du prochain plantage Snort uniquement. Vous pouvez également en générer un si un plantage ne s'est pas produit au cours du dernier jour ou de la semaine. Les vidages de mémoire de Snort 3 sont désactivés par défaut pour les périphériques autonomes. Pour les périphériques à haute disponibilité et en grappe, la fréquence par défaut est désormais une fois par jour. Commandes CLI nouvelles ou modifiées : configure coredump snort3, show coredump Voir : Référence des commandes de défense contre les menaces de Cisco Secure Firewall

Caractéristiques	Version Management Center	Défense Version minimale de Threat Defense	Détails
Capturer les paquets abandonnés avec Cisco Secure Firewall 3100/4200.	7.2.6 7.4.1	7.2.6 (non 4200) 7.4.1	Les pertes de paquets résultant d'incohérences dans le tableau d'adresses MAC peuvent avoir une incidence sur vos capacités de débogage. Le pare-feu Secure Firewall 3100/4200 peut désormais capturer ces paquets abandonnés. Commandes CLI nouvelles ou modifiées : [drop { disable mac-filter }] dans la commande capture. Voir : Référence des commandes de défense contre les menaces de Cisco Secure Firewall

Fonctionnalités obsolètes

Obsolète : téléchargement programmé des versions de maintenance.	7.2.6 7.4.1	N'importe lequel	Incidence sur la mise à niveau. Les tâches de téléchargement planifiées cessent de récupérer les versions de maintenance. La tâche planifiée Télécharger la dernière mise à jour ne télécharge plus les versions de maintenance; désormais, elle télécharge uniquement les derniers correctifs applicables et les mises à jour de VDB. Pour télécharger directement les versions de maintenance (et principales) vers le On-Prem Firewall Management Center, utilisez System (Système)(⚙️) > Product Upgrades (Mises à niveau de produits). Consultez : Automatisation des mises à jour logicielles.
Obsolète : interfaces de confiance de relais DHCP avec FlexConfig.	7.2.6 7.4.1	N'importe lequel	Incidence sur la mise à niveau. Répétez toutes les configurations FlexConfig connexes après la mise à niveau. Vous pouvez désormais utiliser l'interface Web du On-Prem Firewall Management Center pour configurer des interfaces en tant qu'interfaces de confiance afin de conserver l'option 82 de DHCP. Ce faisant, ces paramètres remplacent toutes les configurations FlexConfig existantes, bien que vous deviez les supprimer. Consultez : Configurer les agents de relais DHCP.

Fonctionnalités de On-Prem Firewall Management Center dans la version 7.2.5

Tableau 6 : Fonctionnalités de On-Prem Firewall Management Center dans la version 7.2.5

Caractéristiques	Version minimale Management Center	Défense Version minimale de Threat Defense	Détails
Interfaces			

Caractéristiques	Version minimale Management Center	Défense Version minimale de Threat Defense	Détails
Le centre de gestion détecte les erreurs de synchronisation d'interface.	7.2.5 7.4.1	N'importe lequel	Incidence sur la mise à niveau. Vous devrez peut-être synchroniser les interfaces après la mise à niveau. Dans certains cas, le On-Prem Firewall Management Center peut manquer une configuration pour une interface même si l'interface est correctement configurée et fonctionne sur le périphérique. Si cela se produit et que votre On-Prem Firewall Management Center est en cours d'exécution : • Version 7.2.5 : le déploiement est bloqué jusqu'à ce que vous modifiez le périphérique et synchronisez à partir de la page Interfaces • Versions 7.2.6+/7.4.1+ : le déploiement est autorisé avec un avertissement, mais vous ne pouvez pas modifier les paramètres de l'interface sans synchroniser au préalable. Voir : Synchroniser les modifications à l'interface avec le centre de gestion.

Fonctionnalités de On-Prem Firewall Management Center version 7.2.4

Tableau 7 : Fonctionnalités de On-Prem Firewall Management Center version 7.2.4

Caractéristiques	Version Management Center	Défense Version minimale de Threat Defense	Détails
Fonctionnalités des versions de maintenance antérieures			
Fonctionnalités des versions de maintenance antérieures.	Dépend de la fonctionnalité	Dépend de la fonctionnalité	La version 7.2.4 comporte également : • Incidence sur la mise à niveau Mettre automatiquement à jour les ensembles d'autorités de certification. (7.0.5) • VDB de taille plus restreinte pour les périphériques Snort 2 à faible mémoire. (7.0.6) • Obsolète: alertes d'utilisation élevée du disque non géré. (7.0.6)
Interfaces			

Caractéristiques	Version Management Center	Défense Version minimale de Threat Defense	Détails
La correction d'erreurs directe (FEC) par défaut sur les ports fixes Secure Firewall 3100 a été modifiée, passant de la clause 74 FC-FEC à la clause 108 RS-FEC pour les émetteurs-récepteurs SR, CSR et LR de 25 Gbps et plus.	7.2.4 7.3.0	N'importe lequel	Lorsque vous définissez la FEC sur Auto sur les ports fixes de Cisco Secure Firewall 3100, le type par défaut est désormais l'article 108 RS-FEC au lieu de l'article 74 FC-FEC pour les émetteurs-récepteurs SR, CSR et LR de 25 Go+. Voir : Présentation de l'interface .
Rendement			
Améliorations de la performance du contrôle d'accès (optimisation des objets).	7.2.4 7.4.0	N'importe lequel	Incidence sur la mise à niveau. Le premier déploiement après la mise à niveau du On-Prem Firewall Management Center vers la version 7.2.4 à 7.2.5 ou la version 7.4.0 peut prendre beaucoup de temps et augmenter l'utilisation du processeur sur les périphériques gérés. L'optimisation des objets de contrôle d'accès améliore les performances et consomme moins de ressources de périphérique lorsque vous avez des règles de contrôle d'accès avec des réseaux qui se chevauchent. Les optimisations ont lieu sur le <i>périphérique géré</i> lors du premier déploiement, après l'activation de la fonctionnalité sur On-Prem Firewall Management Center (y compris s'il est activé par une mise à niveau). Si vous avez un grand nombre de règles, le système peut prendre de quelques minutes à une heure pour évaluer vos politiques et effectuer l'optimisation des objets. Pendant ce temps, vous pourriez également constater une utilisation plus élevée du processeur sur vos périphériques. Une situation similaire se produit lors du premier déploiement après la désactivation de la fonctionnalité (y compris si elle est désactivée par la mise à niveau). Une fois cette fonctionnalité activée ou désactivée, nous vous recommandons de la déployer au moment où elle aura le moins d'incidence, comme une fenêtre de maintenance ou une période de faible trafic. Écrans nouveaux ou modifiés (requiert la version 7.2.6) : System (Système)( > Configuration > Access Control Preferences (Préférences de contrôle d'accès) > Object-group optimization (Optimisation des groupes d'objets). Consultez : Préférences de contrôle d'accès

Fonctionnalités de On-Prem Firewall Management Center dans la version 7.2.3

Tableau 8 : Fonctionnalités de On-Prem Firewall Management Center dans la version 7.2.3

Caractéristiques	Version minimale Management Center	Défense Version minimale de Threat Defense	Détails
Firepower 1010E.	7.2.3.1 7.3.1.1 7.4.1	7.2.3 7.4.1	Nous avons lancé le périphérique Firepower 1010E, qui ne prend pas en charge l'alimentation par Ethernet (PoE). N'utilisez pas une version 7.2.3 ou 7.3.0 d'un On-Prem Firewall Management Center pour gérer le périphérique Firepower 1010E. Au lieu de cela, utilisez un On-Prem Firewall Management Center de version 7.2.3.1 et ultérieures ou 7.3.1.1 et ultérieures. Voir : Interfaces de pare-feu standard

On-Prem Firewall Management Center Nouvelles fonctionnalités de la version 7.2.2

Cette version présente des améliorations en matière de stabilité, de renforcement et de performances. Consultez [Bogues résolus dans la version 7.2.2](#), à la page 173.

Fonctionnalités de On-Prem Firewall Management Center dans la version 7.2.1

Tableau 9 : Fonctionnalités de On-Prem Firewall Management Center dans la version 7.2.1

Caractéristiques	Management Center	Défense Version minimale de Threat Defense	Détails
Modules de réseau de contournement matériel (« Fail-to-Wire ») pour Cisco Secure Firewall 3100.	7.2.1 7.3.0	7.2.1	Nous avons introduit ces modules de réseau de contournement matériel pour Cisco Secure Firewall 3130 et 3140 : • Module de réseau de contournement matériel 6 ports 1G SFP, SR (multimode) (FPR-X-NM-6X1SX-F) • Module de réseau de contournement matériel 6 ports 10G SFP, SR (multimode) (FPR-X-NM-6X10SR-F) • Module de réseau de contournement matériel 6 ports 10G SFP, LR (mode unique) (FPR-X-NM-6X10LR-F) • Module de réseau de contournement matériel 6 ports 25G SFP, SR (multimode) (FPR-X-NM-X25SR-F) • Module de réseau de contournement matériel 6 ports 25G, LR (mode unique) (FPR-X-NM-6X25LR-F) • Module de réseau de contournement matériel 8 ports 1G, RJ45 (cuivre) (FPR-X-NM-8X1G-F) Écrans nouveaux ou modifiés : Devices (périphériques) > Device Management (gestion des périphériques) > Interfaces > Edit Physical Interface (modifier l'interface physique) Pour plus de renseignements, consultez Ensembles en ligne et interfaces passives.
Pilote d'adaptateur de réseau Ethernet Intel E810-CQDA2 avec Firewall Threat Defense Virtual pour KVM.	7.2.1 7.3.0	7.2.1	Nous prenons désormais en charge le pilote d'adaptateur de réseau Ethernet Intel E810-CQDA2 avec Firewall Threat Defense Virtual pour KVM. Pour plus de renseignements, consultez Mise en route de Cisco Secure Firewall Threat Defense Virtual et KVM.

Fonctionnalités de On-Prem Firewall Management Center dans la version 7.2.0

Tableau 10 : Fonctionnalités de On-Prem Firewall Management Center dans la version 7.2.0

Caractéristiques	Version minimale Management Center	Défense minimale Version minimale de Threat Defense	Détails
Fonctionnalités des versions de maintenance antérieures			
Fonctionnalités des versions de maintenance antérieures.	Dépend de la fonctionnalité	Dépend de la fonctionnalité	La version 7.2.0 comporte également les fonctionnalités suivantes : • Prise en charge d'ISA 3000 pour l'arrêt. (7.0.2) • Incidence sur la mise à niveau Intégration SecureX et orchestration SecureX améliorées. (7.0.2) • Modifications de l'interface Web : SecureX, informations sur les menaces et autres intégrations. (7.0.2) • Prise en charge de Threat Defense pour Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage). (7.0.3)
Plateforme			
Centre de gestion virtuel pour Alibaba.	7.2.0	N'importe lequel	Nous avons introduit Cisco Secure Firewall Management Center Virtual pour Alibaba Cloud.
Threat defense virtual pour Alibaba.	7.2.0	7.2.0	Nous avons introduit Cisco Secure Firewall Threat Defense pour Alibaba Cloud. Vous devez utiliser le On-Prem Firewall Management Center ; le gestionnaire de périphériques n'est pas pris en charge. Notez qu'en raison de problèmes sous-jacents de l'infrastructure d'Alibaba, le type d'instance virtuelle de Firewall Threat Defense Virtual ecs.g5ne.4xLarge a de faibles performances, en particulier en termes de connexions par seconde (CPS). Nous recommandons le 2xlarge ou 4xlarge.
Les instantanés permettent un déploiement rapide de Firewall Threat Defense Virtual pour AWS et Azure.	7.2.0	7.2.0	Vous pouvez désormais prendre un instantané d'une instance de Firewall Threat Defense Virtual pour AWS ou Azure, puis utiliser cet instantané pour déployer rapidement de nouvelles instances. Cette fonctionnalité améliore également les performances des solutions de mise à l'échelle automatique pour AWS et Azure. Pour obtenir plus d'informations, reportez-vous à la Guide de démarrage de Cisco Secure Firewall Threat Defense Virtual.

Caractéristiques	Version minimale Management Center	Défense minimale Version minimale de Threat Defense	Détails
Mode Analyse pour les périphériques de Firewall Threat Defense gérés dans le nuage.	7.2.0	7.0.3 7.2.0	En même temps que la version 7.2, nous avons introduit le Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), qui utilise la plateforme Cisco Security Cloud Control et unit la gestion de plusieurs solutions de sécurité Cisco. Nous nous assurons des mises à jour des fonctionnalités. Le matériel sur site et les On-Prem Firewall Management Center virtuels exécutant la version 7.2 et versions ultérieures peuvent « cogérer » des périphériques de Firewall Threat Defense gérés dans le nuage, mais à des fins d'analyse et de journalisation des événements uniquement. Vous ne pouvez pas déployer de politique sur ces périphériques à partir d'un On-Prem Firewall Management Center sur site. Écrans nouveaux ou modifiés : - Lorsque vous ajoutez un périphérique géré en nuage à un On-Prem Firewall Management Center sur site, utilisez la nouvelle case à cocher Périphérique géré par CDO pour préciser qu'il est uniquement destiné à l'analyse. - Affichez les périphériques destinés à l'analyse uniquement dans Périphériques > Gestion des périphériques. Commandes CLI nouvelles ou modifiées : configure manager add, configure manager delete, configure manager edit, show managers Pour en savoir plus, consultez Gérer Firewall Threat Defense avec le centre de gestion de pare-feu en nuage Cisco Security Cloud Control.
Haute disponibilité/évolutivité : Threat Defense			

Caractéristiques	Version minimale Management Center	Défense minimale Version minimale de Threat Defense	Détails
Mise en grappe virtuelle pour la Firewall Threat Defense Virtual dans les nuages publics et privés.	7.2.0	7.2.0	Vous pouvez maintenant configurer des grappes pour les plateformes Firewall Threat Defense Virtual suivantes : • Threat Defense Virtual pour AWS : grappes de 16 nœuds • Threat Defense Virtual pour GCP : grappes de 16 nœuds • Threat Defense Virtual pour KVM : grappes de 4 nœuds • Threat Defense Virtual pour VMware : grappes de 4 nœuds Écrans nouveaux ou modifiés : • Périphériques > Gestion des périphériques > Ajouter une grappe • Périphériques > Gestion des périphériques > menu Plus • Périphériques > Gestion des périphériques > Grappe Pour en savoir plus, consultez Mise en grappe Threat Defense Virtual dans un nuage public (AWS, GCP) ou Mise en grappe Threat Defense Virtual dans un nuage privé (KVM, VMware).
Grappes de 16 nœuds pour Firepower 4100/9300 et Firewall Threat Defense Virtual pour AWS et GCP.	7.2.0	7.2.0	Vous pouvez désormais configurer des grappes de 16 nœuds pour Firepower 4100/9300 et Firewall Threat Defense Virtual pour AWS et GCP. Notez que Cisco Secure Firewall 3100 ne prend toujours en charge que 8 nœuds. Pour en savoir plus, consultez Mise en grappe pour Firepower 4100/9300 ou Mise en grappe pour Threat Defense Virtual dans un nuage public.
Haute disponibilité pour Firewall Threat Defense Virtual pour Nutanix.	7.2.0	7.2.0	Nous prenons désormais en charge la haute disponibilité pour Firewall Threat Defense Virtual pour Nutanix. Pour obtenir plus d'informations, reportez-vous à la Guide de démarrage de Cisco Secure Firewall Threat Defense Virtual.
Mise à l'échelle automatique de Firewall Threat Defense Virtual pour les équilibreurs de charge de passerelle AWS.	7.2.0	7.2.0	Nous prenons désormais en charge l'évolutivité automatique pour Firewall Threat Defense Virtual pour les équilibreurs de charge de passerelle AWS, à l'aide d'un modèle CloudFormation. Pour obtenir plus d'informations, reportez-vous à la Guide de démarrage de Cisco Secure Firewall Threat Defense Virtual.

Caractéristiques	Version minimale Management Center	Défense minimale Version minimale de Threat Defense	Détails
Mise à l'échelle automatique pour Firewall Threat Defense Virtual pour GCP.	7.2.0	7.2.0	Incidence sur la mise à niveau. Les mises à niveau de Threat Defense Virtual pour Google Cloud Platform (GCP) ne peuvent pas dépasser la version 7.2.0. Nous prenons désormais en charge l'évolutivité automatique des instances Firewall Threat Defense Virtual pour GCP, en positionnant un groupe d'instances Firewall Threat Defense Virtual entre un équilibreur de charge interne (ILB) de GCP et un équilibreur de charge externe (ELB) de GCP. Restrictions de version : en raison des modifications de l'interface requises pour prendre en charge cette fonctionnalité, Firewall Threat Defense Virtual dans le cadre des mises à niveau de Google Cloud Platform ne peut pas dépasser la version 7.2.0. C'est-à-dire que vous ne pouvez pas mettre à niveau vers la version 7.2.0+ à partir de la version 7.1.x ou des versions antérieures. Vous devez déployer une nouvelle instance et refaire toutes les configurations propres au périphérique. Pour obtenir plus d'informations, reportez-vous à la Guide de démarrage de Cisco Secure Firewall Threat Defense Virtual.
Interfaces			
Prise en charge de LLDP pour Firepower 2100 et Secure Firewall 3100.	7.2.0	7.2.0	Vous pouvez maintenant activer le protocole LLDP (Link Layer Discovery Protocol) pour les interfaces Firepower 2100 et Secure Firewall 3100. Écrans nouveaux ou modifiés : Périphériques > Gestion des périphériques > Interfaces > Configuration du matériel > LLDP Commandes nouvelles ou modifiées : show lldp status, show lldp neighbors, show lldp statistics Pour en savoir plus, reportez-vous à la présentation des interfaces.
Suspendez les trames pour le contrôle de flux pour Secure Firewall 3100.	7.2.0	7.2.0	S'il y a une rafale de trafic, des paquets abandonnés peuvent se produire si la rafale dépasse la capacité de mise en mémoire tampon de la mémoire tampon FIFO sur la carte réseau et les mémoires tampons des anneaux de réception. L'activation des trames de pause pour le contrôle de flux peut atténuer ce problème. Écrans nouveaux ou modifiés : Périphériques > Gestion des périphériques > Interfaces > Configuration du matériel > Connectivité réseau Pour en savoir plus, reportez-vous à la présentation des interfaces.

Caractéristiques	Version minimale Management Center	Défense minimale Version minimale de Threat Defense	Détails
Ports d'éclatement pour Cisco Secure Firewall 3130 et 3140.	7.2.0	7.2.0	Vous pouvez maintenant configurer quatre ports d'éclatement de 10 Go pour chaque interface de 40 Go sur les Cisco Secure Firewall 3130 et 3140. Écrans nouveaux ou modifiés : Périphériques > Gestion des périphériques > Opérations du châssis. Pour en savoir plus, reportez-vous à la présentation des interfaces.
Configurez VXLAN à partir de l'interface Web du On-Prem Firewall Management Center.	7.2.0	N'importe lequel	Incidence sur la mise à niveau. Rétablir FlexConfigs après la mise à niveau. Vous pouvez maintenant utiliser l'interface Web du On-Prem Firewall Management Center pour configurer les interfaces VXLAN. Les VXLAN agissent comme réseau virtuel de couche 2 sur un réseau physique de couche 3 pour étendre le réseau de couche 2. Si vous avez configuré les interfaces VXLAN avec FlexConfig dans une version précédente, elles continuent de fonctionner. En fait, FlexConfig prévaut dans ce cas : si vous refaites vos configurations VXLAN dans l'interface Web, supprimez les paramètres FlexConfig. Écrans nouveaux ou modifiés : • Configurez l'interface source du VTEP : Périphériques > , Gestion des périphériques > VTEP • Configurer l'interface VNI : Périphériques > Gestion des périphériques > Interfaces > Ajouter une interface VNI Pour en savoir plus, consultez Interfaces de pare-feu standard.
NAT			
Activer, désactiver ou supprimer plusieurs règles NAT à la fois.	7.2.0	N'importe lequel	Vous pouvez sélectionner plusieurs règles NAT et les activer, les désactiver ou les supprimer en même temps. Activez et désactivez l'option Appliquer aux règles NAT manuelles uniquement, tandis que la suppression s'applique à toutes les règles NAT. Pour en savoir plus, consultez Traduction d'adresses réseau.
VPN			

Caractéristiques	Version minimale Management Center	Défense minimale Version minimale de Threat Defense	Détails
Certificat et authentification SAML pour les profils de connexion de VPN d'accès à distance.	7.2.0	7.2.0	Nous prenons désormais en charge les certificats et l'authentification SAML pour les profils de connexion de VPN d'accès à distance. Vous pouvez authentifier un certificat d'ordinateur ou un certificat utilisateur avant qu'une authentification ou une autorisation SAML ne soit lancée. Cela peut être fait à l'aide des attributs de certificat DAP ainsi que des attributs DAP SAML spécifiques à l'utilisateur. Écrans nouveaux ou modifiés : vous pouvez désormais choisir l'option de certificat et SAML lors du choix de la méthode d'authentification pour le profil de connexion dans une politique de VPN d'accès à distance. Pour en savoir plus, consultez VPN d'accès à distance.
VPN de site à site basé sur le routage avec topologie de concentrateur en étoile.	7.2.0	7.2.0	Nous avons ajouté la prise en charge des VPN de site à site basés sur le routage dans une topologie en étoile. Auparavant, cette topologie ne prenait en charge que les VPN basés sur les politiques (carte de chiffrement). Écrans nouveaux ou modifiés : lorsque vous ajoutez une nouvelle topologie VPN et choisissez Route Based (VTI), vous pouvez désormais également choisir Hub and Spoke (en étoile). Pour en savoir plus, consultez VPN de site à site.
Décharge de flux IPsec pour Secure Firewall 3100.	7.2.0	7.2.0	Sur le pare-feu Secure Firewall 3100, les flux IPsec sont déchargés par défaut. Après la configuration initiale d'une association de sécurité (SA), d'un VPN de site à site ou d'un VPN d'accès à distance IPsec, les connexions IPsec sont déchargées vers le FPGA (field programmable gate RAID) dans le périphérique, ce qui devrait améliorer les performances du périphérique. Vous pouvez modifier la configuration à l'aide de FlexConfig et de la commande flow-offload-ipsec. Pour en savoir plus, consultez VPN de site à site.

Routing (Routage)

Caractéristiques	Version minimale Management Center	Défense minimale Version minimale de Threat Defense	Détails
Configurer le protocole EIGRP à partir de l'interface Web du On-Prem Firewall Management Center.	7.2.0	N'importe lequel	Incidence sur la mise à niveau. Rétablir FlexConfigs après la mise à niveau. Vous pouvez maintenant utiliser l'interface Web du On-Prem Firewall Management Center pour configurer EIGRP. Notez que vous ne pouvez activer le protocole EIGRP que sur les interfaces appartenant au routeur virtuel global du périphérique. Si vous avez configuré le protocole EIGRP avec FlexConfig dans une version précédente, le système vous permet de déployer après la mise à niveau, mais vous invite également à refaire vos configurations EIGRP dans l'interface Web. Lorsque vous êtes satisfait de la nouvelle configuration, vous pouvez supprimer les objets ou les commandes FlexConfig obsolètes. Pour vous aider dans ce processus, nous fournissons un outil de migration de ligne de commande. Écrans nouveaux ou modifiés : Périphériques > Gestion des périphériques > Routage > EIGRP Pour en savoir plus, consultez EIGRP et Migration des politiques FlexConfig.
Prise en charge de routeurs virtuels pour la Firepower 1010.	7.2.0	7.2.0	Vous pouvez maintenant configurer jusqu'à cinq routeurs virtuels sur le Firepower 1010. Pour en savoir plus, consultez la section Routeurs virtuels.
Prise en charge des VTI dans les routeurs virtuels définis par l'utilisateur.	7.2.0	7.2.0	Vous pouvez désormais affecter des interfaces de tunnel virtuel aux routeurs virtuels définis par l'utilisateur. Auparavant, vous ne pouviez affecter des VTI qu'aux routeurs virtuels mondiaux. Écrans nouveaux ou modifiés : Devices (Périphériques) > Device Management (Gestion des périphériques) > Routing (Routage) > Virtual Router Properties (Propriétés du routeur virtuel) Pour en savoir plus, consultez la section Routeurs virtuels.

Caractéristiques	Version minimale Management Center	Défense minimale Version minimale de Threat Defense	Détails
Routage basé sur des politiques avec surveillance du chemin d'accès.	7.2.0	7.2.0	Vous pouvez désormais utiliser la surveillance des chemins pour recueillir les mesures de performance (RTT, gigue, pertes de paquets et MOS) des interfaces de sortie d'un périphérique. Vous pouvez ensuite utiliser ces mesures pour déterminer le meilleur chemin pour le routage basé sur les politiques. Écrans nouveaux ou modifiés : • Activez la surveillance des chemins d'accès et choisissez les mesures à collecter : Périphériques > Gestion des périphériques > Interfaces > Surveillance du chemin • Utilisez la nouvelle option d'ordre d'interface lorsque vous ajoutez un routage basé sur une politique et que vous spécifiez une action de transfert : Périphériques > Gestion des périphériques > Routage > Routage basé sur une politique • Surveillez les mesures du chemin dans le tableau de bord de surveillance de l'état d'intégrité de chaque périphérique : System (système)(⚙️) > Health (intégrité) > Monitor (moniteur) > add dashboard (ajouter un tableau de bord) > Interface - Path Metrics (interface - mesures du chemin). Commandes CLI nouvelles ou modifiées : show policy route, show path-monitoring, clear path-monitoring Pour en savoir plus, consultez Routage basé sur des politiques.
Informations sur les menaces			
Informations sur les menaces basées sur le DNS de Cisco Umbrella.	7.2.0	N'importe lequel	Nous prenons désormais en charge les renseignements sur la sécurité basés sur le DNS à l'aide d'informations régulièrement mises à jour de Cisco Umbrella. Vous pouvez utiliser une politique DNS locale et une politique Cisco Cisco Umbrella DNS pour obtenir deux couches de protection. Écrans nouveaux ou modifiés : • Configurer la connexion à Umbrella : Intégration > Autres intégrations > Services en nuage > Connexion Cisco Umbrella • Configurer la politique Cisco Umbrella DNS : Politiques > DNS > Ajouter une politique DNS > Politique DNA Umbrella • Associer la politique Cisco Umbrella DNS au contrôle d'accès : Politiques (Politiques) > Access Control (Contrôle d'accès) > Edit Policy (Modifier la politique) > Security Intelligence (Renseignements de sécurité) > Umbrella DSN Policy (Politique Umbrella DNS) Pour en savoir plus, consultez Politiques DNS.

Caractéristiques	Version minimale Management Center	Défense minimale Version minimale de Threat Defense	Détails
Informations sur les menaces basées sur l'IP d'Amazon GuardDuty.	7.2.0	N'importe lequel	Vous pouvez désormais gérer le trafic en fonction d'adresses IP malveillantes détectées par Amazon GuardDuty, lors de l'intégration au centre de gestion virtuel pour AWS. Le système utilise ces informations sur les menaces par l'intermédiaire d'un flux d'informations de sécurité personnalisé ou d'un groupe d'objets réseau régulièrement mis à jour, que vous pouvez ensuite utiliser dans vos politiques de sécurité. Pour obtenir plus d'informations, reportez-vous à la Guide de démarrage de Cisco Secure Firewall Threat Defense Virtual.

Contrôle d'accès : détection des menaces et identification des applications

Gestion dynamique des objets avec : • Connecteur d'attributs dynamiques Cisco Secure en nuage • Connecteur d'attributs dynamiques Cisco Secure 2.0 sur site	7.2.0	N'importe lequel	En même temps que la version 7.2, nous avons publié les mises à jour suivantes pour le connecteur Cisco Secure Dynamic Attributes : • Cisco Secure Dynamic Attributes Connector en nuage (service géré par Security Cloud Control) Les On-Prem Firewall Management Center pris en charge : version 7.1 et ultérieures et le On-Prem Firewall Management Center en mode cloud. Charges de travail virtuelles ou en nuage prises en charge : AWS, Azure, balises de service Azure, Google Cloud Connector, GitHub et Office 365. <i>Gestion du connecteur d'attributs dynamiques Cisco Secure avec Cisco Security Cloud Control</i> chapitres dans Gérer Firewall Threat Defense avec le centre de gestion de pare-feu en nuage Cisco Security Cloud Control Pour en savoir plus : • Connecteur d'attributs dynamiques Cisco Secure 2.0 sur site Les On-Prem Firewall Management Center pris en charge : version 7.0+ et le On-Prem Firewall Management Center en mode cloud. Charges de travail virtuelles ou en nuage prises en charge : AWS, Azure, balises de service Azure, Google Cloud Connector, GitHub, Office 365 et VMware. Pour de plus amples renseignements : Guide de configuration du connecteur d'attributs dynamiques Cisco Secure 2.0
---	-------	------------------	--

Caractéristiques	Version minimale Management Center	Défense minimale Version minimale de Threat Defense	Détails
Contournez les flux d'inspection ou d'éléphants sur les périphériques Snort 3.	7.2.0	7.2.0 avec Snort 3	Vous pouvez désormais détecter et éventuellement contourner les flux d'inspection ou de limitation des éléphants. Par défaut, les politiques de contrôle d'accès sont définies pour générer un événement lorsque le système détecte une connexion non chiffrée supérieure à 1 Go/10 sec. la limite de débit est configurable. Pour les périphériques Firepower 2100, vous pouvez détecter les flux d'éléphants, mais pas contourner l'inspection ou la limitation. Pour les périphériques exécutant Snort 2 et pour les périphériques exécutant la version 7.1 ou une version antérieure, continuez à utiliser Intelligent Application Bypass (IAB). Écrans nouveaux ou modifiés : nous avons ajouté les paramètres de flux d'éléphants à l'onglet Avancé de la politique de contrôle d'accès. Pour en savoir plus, consultez la page relative à la détection de flux d'éléphants.

Caractéristiques	Version minimale Management Center	Défense minimale Version minimale de Threat Defense	Détails															
Améliorations au moteur de visibilité chiffrée (EVE)	7.2.0	7.2.0 avec Snort 3	Nous avons apporté les améliorations suivantes au moteur de visibilité chiffrée (EVE) : • La fonctionnalité Encrypted Visibility Engine (Moteur de visibilité chiffrée) peut détecter le système d’exploitation utilisé par l’hôte, qui est signalé dans les événements et la cartographie du réseau. • La fonctionnalité Encrypted Visibility Engine (Moteur de visibilité chiffrée) peut détecter le trafic d’application en attribuant aux applications des processus EVE qui ont été identifiés avec un niveau de confiance élevé, que vous pouvez ensuite utiliser dans les règles de contrôle d’accès pour contrôler le trafic réseau. (Dans la version 7.1, vous pouviez voir les processus EVE pour les connexions, mais vous ne pouviez pas agir sur la base de ces connaissances.) Pour ajouter des affectations supplémentaires, créez des applications personnalisées ou des détecteurs d’applications personnalisés. Lorsque vous ajoutez un schéma de détection à votre détecteur personnalisé, choisissez Encrypted Visibility Engine (moteur de visibilité chiffrée) comme application. Spécifiez ensuite le nom du processus et le niveau de confiance. • La fonctionnalité Encrypted Visibility Engine (Moteur de visibilité chiffrée) fonctionne maintenant avec le trafic QUIC. Les champs d'événement de connexion suivants ont été modifiés en fonction de ces améliorations : <table><tr><td>Nom du processus d'empreinte digitale TLS</td><td>est ~~maintenant~~</td><td>Nom du processus de visibilité chiffrée</td></tr><tr><td>Score de confiance du processus d'empreintes digitales TLS</td><td>est ~~maintenant~~</td><td>Note de confiance du processus de visibilité chiffrée</td></tr><tr><td>Confiance dans les maliciels de l’empreinte digitale TLS</td><td>est ~~maintenant~~</td><td>Niveau de confiance des menaces pour la visibilité chiffrée</td></tr><tr><td>Score de confiance des maliciels de l’empreinte digitale TLS</td><td>est ~~maintenant~~</td><td>Note de confiance des menaces pour la visibilité chiffrée</td></tr><tr><td>Type de détection : empreinte TLS</td><td>est ~~maintenant~~</td><td>Type de détection : visibilité chiffrée</td></tr></table> Cette fonctionnalité requiert une licence Threat. Pour en savoir plus, consultez Politiques de contrôle d’accès et Détection d’applications.	Nom du processus d'empreinte digitale TLS	est ~~maintenant~~	Nom du processus de visibilité chiffrée	Score de confiance du processus d'empreintes digitales TLS	est ~~maintenant~~	Note de confiance du processus de visibilité chiffrée	Confiance dans les maliciels de l’empreinte digitale TLS	est ~~maintenant~~	Niveau de confiance des menaces pour la visibilité chiffrée	Score de confiance des maliciels de l’empreinte digitale TLS	est ~~maintenant~~	Note de confiance des menaces pour la visibilité chiffrée	Type de détection : empreinte TLS	est ~~maintenant~~	Type de détection : visibilité chiffrée
Nom du processus d'empreinte digitale TLS	est ~~maintenant~~	Nom du processus de visibilité chiffrée																
Score de confiance du processus d'empreintes digitales TLS	est ~~maintenant~~	Note de confiance du processus de visibilité chiffrée																
Confiance dans les maliciels de l’empreinte digitale TLS	est ~~maintenant~~	Niveau de confiance des menaces pour la visibilité chiffrée																
Score de confiance des maliciels de l’empreinte digitale TLS	est ~~maintenant~~	Note de confiance des menaces pour la visibilité chiffrée																
Type de détection : empreinte TLS	est ~~maintenant~~	Type de détection : visibilité chiffrée																

Caractéristiques	Version minimale Management Center	Défense minimale Version minimale de Threat Defense	Détails
Inspection TLS 1.3	7.2.0	7.2.0 avec Snort 3	Nous prenons désormais en charge l'inspection du trafic TLS 1.3. Écrans nouveaux ou modifiés : nous avons ajouté l'option Enable TLS 1.3 Decryption (Activer le déchiffrement TLS 1.3) à l'onglet Advanced Settings (Paramètres avancés) des politiques SSL. Veuillez noter que cette option est désactivée par défaut. Pour en savoir plus, consultez Politiques SSL.
Amélioration de la détection des balayages de ports.	7.2.0	7.2.0 avec Snort 3	Grâce au détecteur de balayage de ports amélioré, vous pouvez facilement configurer le système pour détecter ou empêcher le balayage de ports. Vous pouvez affiner les réseaux que vous souhaitez protéger, définir la sensibilité, etc. Pour les périphériques exécutant Snort 2 et pour les périphériques exécutant la version 7.1 ou antérieure, continuez à utiliser la politique d'analyse de réseau pour la détection par balayage de ports. Écrans nouveaux ou modifiés : nous avons ajouté Détection des menaces à l'onglet Avancé de la politique de contrôle d'accès. Pour en savoir plus, consultez Détection des menaces.
Inspection des macros VBA	7.2.0	7.2.0 avec Snort 3	Nous prenons désormais en charge l'inspection des macros VBA (Visual Basic pour Applications) dans les documents Microsoft Office, qui se fait par décompression des macros et des règles de correspondance en fonction du contenu décompressé. Par défaut, la décompression des macros VBA est désactivée dans toutes les politiques d'analyse de réseau fournies par le système. Pour l'activer, utilisez le paramètre <code>decompress_vba</code> dans les inspecteurs imap, smtp, http_inspect et pop Snort 3. Pour configurer des règles de prévention des intrusions personnalisées en fonction des macros décompressées, utilisez l'option <code>vba_data</code>. Pour obtenir des renseignements supplémentaires, consultez le Référence de l'inspecteur Snort 3 et le Guide de configuration Snort 3 de Cisco Secure Firewall Management Center.

Caractéristiques	Version minimale Management Center	Défense minimale Version minimale de Threat Defense	Détails
Amélioration de l'inspection de JavaScript.	7.2.0	7.2.0 avec Snort 3	Nous avons amélioré l'inspection de JavaScript, qui s'effectue en normalisant JavaScript et des règles de mise en correspondance en fonction du contenu normalisé. Les améliorations d'un nouveau normalisateur comprennent une normalisation améliorée des espaces, des insertions de points-virgules, la gestion des scripts intersites, la normalisation et la modification des alias des identifiants, l'inspection juste à temps (JIT) et la possibilité d'inspecter les scripts externes. Par défaut, le nouveau normalisateur est activé dans toutes les politiques d'analyse de réseau fournies par le système. Pour modifier les performances ou désactiver la fonctionnalité dans une politique d'analyse de réseau personnalisée, utilisez les paramètres <code>js_norm</code> (normalisateur amélioré) et <code>normalize_javascript</code> (normalisateur existant) dans l'inspecteur <code>https_inspect</code> de Snort 3. Pour configurer des règles de prévention des intrusions personnalisées en fonction de JavaScript normalisé, utilisez l'option <code>js_data</code>, par exemple : <pre>alert tcp any any -> any any (msg:"Script detected!"; js_data; content:"var var_0000=1;"; sid:1000001;)</pre> Pour en savoir plus, consultez HTTP Inspect Inspector dans le Référence de l'inspecteur Snort 3, ainsi que le Guide de configuration Snort 3 de Cisco Secure Firewall Management Center.
Inspection SMB 3 améliorée.	7.2.0	7.2.0 avec Snort 3	Nous prenons désormais en charge l'inspection du trafic SMB 3 dans les situations suivantes : • Pendant le basculement du nœud du serveur de fichiers pour les grappes configurées pour le basculement transparent SMB. • Dans plusieurs nœuds de serveur de fichiers pour les grappes utilisant l'évolutivité horizontale de SMB. • Par le biais de modifications des renseignements d'annuaire en raison de la location d'annuaire de SMB. • Répartis sur plusieurs connexions en raison du multicanal SMB. Pour obtenir des renseignements supplémentaires, consultez le Référence de l'inspecteur Snort 3 et le Guide de configuration Snort 3 de Cisco Secure Firewall Management Center.

Journalisation et analyse des événements

Caractéristiques	Version minimale Management Center	Défense minimale Version minimale de Threat Defense	Détails
Connecter les événements de sécurité à plusieurs entrepôts de données sur site de Cisco Secure Network Analytics.	7.2.0	7.0.0	Lorsque vous configurez une intégration du magasin de données Cisco Secure Network Analytics (nœuds multiples), vous pouvez désormais ajouter plusieurs collecteurs de flux pour les événements de sécurité. Vous affectez chaque collecteur de flux à un ou plusieurs périphériques de Firewall Threat Defense exécutant la version 7.0 et ultérieures. Écrans nouveaux ou modifiés : • Configuration : Intégration > Security Analytics & Logging > Magasin de données de Cisco Secure Network Analytics • Modification : intégration > Security Analytics & Logging > Mettre à jour les affectations de périphériques Cette fonction nécessite Cisco Secure Network Analytics version 7.1.4. Pour obtenir plus d'informations, reportez-vous à la Cisco Security Analytics and Logging (On Premises) : Guide d'intégration des événements de pare-feu.
L'accès à la base de données a été modifié.	7.2.0	N'importe lequel	Nous avons ajouté dix nouvelles tables, rendu une table obsolète et interdit les jonctions dans six tables. Nous avons également ajouté des champs à divers tableaux pour la prise en charge de Snort 3 et pour fournir les horodatages et les adresses IP dans un format lisible par l'homme. Pour en savoir plus, consultez la rubrique <i>Nouveautés</i> dans le Guide d'accès à la base de données de Cisco Secure Firewall Management Center, version 7.2.
eStreamer a été modifié.	7.2.0	N'importe lequel	Un nouveau client de référence basé sur Python a été ajouté au SDK. En outre, vous pouvez désormais demander des événements complets. Pour en savoir plus, consultez la rubrique <i>What's New (Nouveautés)</i> dans le Guide d'intégration des flux continus d'événements de Cisco Secure Firewall Management Center, version 7.2.

Déploiement et gestion des politiques

Caractéristiques	Version minimale Management Center	Défense minimale Version minimale de Threat Defense	Détails
Restauration automatique d'un déploiement qui entraîne une perte de la connectivité de gestion.	7.2.0	7.2.0	Vous pouvez désormais activer la restauration automatique de la configuration si un déploiement entraîne l'arrêt de la connexion de gestion entre le On-Prem Firewall Management Center et Firewall Threat Defense. Auparavant, vous ne pouviez restaurer manuellement une configuration qu'à l'aide de la commande configure policy rollback. Écrans nouveaux ou modifiés : • Périphériques > Gestion des périphériques > Périphérique > Paramètres de déploiement • Déployer > Déploiement avancé > Prévisualiser • Déployer > Historique du déploiement > Prévisualiser Pour plus d'informations, consultez Gestion des périphériques.
Générer un rapport et envoyez-le par courriel lorsque vous déployez des modifications de configuration.	7.2.0	N'importe lequel	Vous pouvez désormais générer un rapport pour n'importe quelle tâche de déploiement. Le rapport contient des détails sur la configuration déployée. Pages nouvelles ou modifiées : Déployer > Historique de déploiement (🔍) icône > Plus (⚙️) Générer un rapport Pour plus de renseignements, consultez Déploiement de configuration.
Verrouillage des politiques de contrôle d'accès	7.2.0	N'importe lequel	Vous pouvez désormais verrouiller une politique de contrôle d'accès pour empêcher d'autres administrateurs de la modifier. Le verrouillage de la politique garantit que vos modifications ne seront pas invalidées si un autre administrateur modifie la politique et enregistre les modifications avant vous. Tout utilisateur qui est autorisé à modifier la politique de contrôle d'accès a l'autorisation de la verrouiller. Nous avons ajouté une icône pour verrouiller ou déverrouiller une politique à côté de son nom lors de la modification de celle-ci. De plus, il existe une nouvelle autorisation pour permettre aux utilisateurs de déverrouiller les politiques verrouillées par d'autres administrateurs : remplacer le verrouillage de la politique de contrôle d'accès. Cette autorisation est activée par défaut dans les rôles Administrateur, Administrateur de l'accès et Administrateur réseau. Pour en savoir plus, consultez Politiques de contrôle d'accès.

Caractéristiques	Version minimale Management Center	Défense minimale Version minimale de Threat Defense	Détails
La recherche de groupe d'objets est activée par défaut.	7.2.0	N'importe lequel	Le paramètre de Object Group Search (Recherche dans les groupes d'objets) est maintenant activé par défaut lorsque vous ajoutez un périphérique au On-Prem Firewall Management Center. Écrans nouveaux ou modifiés : Périphériques > Gestion des périphériques > Périphérique > Paramètres avancés Pour plus d'informations, consultez Gestion des périphériques.
Le nombre de résultats des règles de contrôle d'accès persiste pendant le redémarrage.	7.2.0	7.2.0	Le redémarrage d'un périphérique géré ne réinitialise plus le nombre de résultats de règles de contrôle d'accès à zéro. Le nombre de résultats est réinitialisé uniquement si vous effacez activement les compteurs. En outre, les décomptes sont gérés séparément par chaque unité d'une paire ou d'une grappe à haute disponibilité. Vous pouvez utiliser la commande show rule hits pour afficher les compteurs cumulés pour la paire ou la grappe à haute disponibilité, ou pour voir le nombre par nœud. Commandes CLI nouvelles ou modifiées : show rule hits Pour obtenir plus d'informations, reportez-vous à la Référence des commandes de défense contre les menaces de Cisco Secure Firewall.
Nouvelle interface utilisateur la stratégie de contrôle d'accès.	7.2.0	N'importe lequel	Une nouvelle interface utilisateur expérimentale est disponible pour la stratégie de contrôle d'accès. Vous pouvez continuer à utiliser l'interface utilisateur existante ou essayer la nouvelle interface utilisateur. La nouvelle interface comporte à la fois un affichage sous forme de tableau et de grille pour la liste de règles, la capacité d'afficher ou de masquer des colonnes, une recherche améliorée, un défilement sans fin, une vue plus claire du flux de paquets lié aux politiques associées à la politique de contrôle d'accès, et une fonction ajouter/modifier la boîte de dialogue pour créer des règles. Vous pouvez facilement basculer entre la nouvelle et l'ancienne interface utilisateur lors de la modification d'une politique de contrôle d'accès. Remarque La nouvelle interface ne comporte pas toutes les fonctionnalités disponibles dans l'interface existante et peut se heurter à des problèmes de performance lors de l'affichage d'un grand nombre de règles. Si vous rencontrez des problèmes avec la nouvelle interface utilisateur, revenez à l'ancienne. De plus, Centre d'assistance technique Cisco (TAC) apprécie vos commentaires. Si votre entreprise le permet, vous pouvez nous aider à améliorer cette fonctionnalité en vous assurant que l'analyse Web est activée : Système (⚙) > Configuration > Web Analytics (analyse Web). Pour en savoir plus, consultez Politiques de contrôle d'accès.

Mise à jour

Caractéristiques	Version minimale Management Center	Défense minimale Version minimale de Threat Defense	Détails
Copier les paquets de mise à niveau (« synchronisation homologue à homologue ») d'un appareil à l'autre.	7.2.0	7.2.0	Au lieu de copier les paquets de mise à niveau sur chaque périphérique à partir de On-Prem Firewall Management Center ou du serveur Web interne, vous pouvez utiliser l'interface de ligne de commande Firewall Threat Defense pour copier les paquets de mise à niveau entre les périphériques (« synchronisation homologue à homologue »). Ce partage de ressources sécurisé et fiable passe par le réseau de gestion, mais ne repose pas sur On-Prem Firewall Management Center. Chaque périphérique peut accueillir 5 transferts simultanés de paquets. Cette fonctionnalité est prise en charge pour les périphériques autonomes de la version 7.2.x–7.4.x gérés par le même On-Prem Firewall Management Center de la version autonome 7.2.x–7.4.x. Elle n'est pas prise en charge pour : • Instances de conteneur. • Paires et grappes de périphériques à haute disponibilité. Ces périphériques reçoivent le paquet les uns des autres dans le cadre de leur processus de synchronisation normal. La copie de l'ensemble de mises à niveau sur un membre du groupe la synchronise automatiquement avec tous les membres du groupe. • Périphériques gérés par des On-Prem Firewall Management Center à haute disponibilité. • Périphériques dans différents domaines, ou périphériques séparés par une passerelle NAT. • Périphériques mis à niveau à partir de la version 7.1 ou d'une version antérieure, quelle que soit la version de On-Prem Firewall Management Center. • Périphériques exécutant la version 7.6+. Commandes CLI nouvelles ou modifiées : configure p2psync enable, configure p2psync disable, show peers, show peer details, sync-from-peer, show p2p-sync-status

Caractéristiques	Version minimale Management Center	Défense minimale Version minimale de Threat Defense	Détails
Mise à niveau automatique vers Snort 3 après une mise à niveau réussie de la Firewall Threat Defense.	7.2.0	7.2.0	Lorsque vous utilisez un On-Prem Firewall Management Center de la version 7.2+ pour mettre à niveau Firewall Threat Defense à la version 7.2 ou ultérieure, vous pouvez désormais choisir de mettre à niveau Snort 2 vers Snort 3. Après la mise à niveau logicielle, les périphériques admissibles seront mis à niveau de Snort 2 vers Snort 3 lorsque vous déployez des configurations. Pour les périphériques qui ne sont pas admissibles, car ils utilisent des stratégies d'intrusion ou d'analyse de réseau personnalisées, nous vous recommandons fortement de mettre à niveau manuellement Snort 3 pour une détection et une amélioration améliorées. Pour obtenir de l'aide, consultez Guide de configuration Cisco Secure Firewall Management Center pour Snort 3 pour votre version. Restrictions de version : non pris en charge pour les mises à niveau de Firewall Threat Defense vers la version 7.0.x ou 7.1.x..
Mise à niveau pour les grappes à un seul nœud.	7.2.0	N'importe lequel	Vous pouvez désormais utiliser la page de mise à niveau des périphériques (Périphériques > Mise à niveau de périphériques) pour mettre à niveau les grappes avec un seul nœud actif. Tous les nœuds désactivés sont également mis à niveau. Auparavant, ce type de mise à niveau échouait. Cette fonction n'est pas prise en charge à partir de la page des mises à jour du système (System (Système) > Updates (Mises à jour)). Les mises à niveau rapides ne sont pas non plus prises en charge dans ce cas. Les interruptions du flux de trafic et de l'inspection dépendent des configurations d'interface de la seule unité active, tout comme pour les périphériques autonomes. Plateformes prises en charge : Firepower 4100/9300, Secure Firewall 3100

Caractéristiques	Version minimale Management Center	Défense minimale Version minimale de Threat Defense	Détails
Annulation des mises à niveau de la Firewall Threat Defense à partir de l'interface CLI.	7.2.0	7.2.0	Vous pouvez désormais annuler les mises à niveau de la Firewall Threat Defense à partir de l'interface de ligne de commande du périphérique si les communications entre le On-Prem Firewall Management Center et le périphérique sont interrompues. Notez que dans les déploiements à haute disponibilité et évolutivité, la restauration est plus réussie lorsque toutes les unités sont restaurées simultanément. Lors du rétablissement à l'aide de l'interface de ligne de commande, ouvrez des sessions avec toutes les unités, vérifiez que le rétablissement est possible sur chacune, puis démarrez les processus en même temps. Mise en garde Le fait de revenir de l'interface de ligne de commande peut entraîner la désynchronisation des configurations entre le périphérique et le On-Prem Firewall Management Center, en fonction de ce que vous avez modifié après la mise à niveau. Cela peut entraîner d'autres problèmes de communication et de déploiement. Commandes CLI nouvelles ou modifiées : upgrade revert, show upgrade revert-info. Pour en savoir plus, consultez Annulation de la mise à niveau.
Administration			
Plusieurs groupes de serveurs DNS pour résoudre les requêtes DNS.	7.2.0	N'importe lequel	Vous pouvez configurer plusieurs groupes DNS pour la résolution des requêtes DNS des systèmes clients. Vous pouvez utiliser ces groupes de serveurs DNS pour résoudre les demandes concernant différents domaines DNS. Par exemple, vous pouvez avoir un groupe par défaut "fourre-tout" qui utilise des serveurs DNS publics, pour les connexions à l'internet. Vous pouvez ensuite configurer un groupe distinct pour utiliser les serveurs DNS internes pour le trafic interne, par exemple, toute connexion à une machine du domaine exemple.com. Ainsi, les connexions à un nom de domaine complet utilisant le nom de domaine de votre organisation seront résolues à l'aide de vos serveurs DNS internes, tandis que les connexions à des serveurs publics utiliseront des serveurs DNS externes. Écrans nouveaux ou modifiés : Paramètres de la plateforme > DNS Pour en savoir plus, consultez Paramètres de la plateforme.

Caractéristiques	Version minimale Management Center	Défense minimale Version minimale de Threat Defense	Détails															
Configurez la validation des certificats avec Firewall Threat Defense par type d'utilisation.	7.2.0	7.2.0	Vous pouvez maintenant préciser les types d'utilisation où la validation est autorisée avec le point de confiance (le périphérique de Firewall Threat Defense) : connexions client IPsec, connexions client SSL et certificats de serveur SSL. Écrans nouveaux ou modifiés : nous avons ajouté une option de validation de l'utilisation aux objets d'inscription de certificat : Objets > Gestionnaire d'objets > PKI > Inscription du certificat. Pour en savoir plus, consultez Gestion des objets.															
Option de français pour l'interface Web.	7.2.0	N'importe lequel	Vous pouvez maintenant faire basculer l'interface Web du On-Prem Firewall Management Center en français. Nouveaux écrans ou modifiés : Système (⚙️) Configuration > Langues Pour plus d'informations, voir Configuration du système.															
Modifications de l'interface Web : intégration de déploiement et de l'activité des utilisateurs	7.2.0	N'importe lequel	La version 7.2 modifie toujours ces options de menu du On-Prem Firewall Management Center. <table><tr><td>Déployer > Historique de déploiement</td><td>est maintenu</td><td>Déployer > Historique de déploiement (🔍) (coin inférieur droit)</td></tr><tr><td>Déployer > Déploiement</td><td>est maintenu</td><td>Déploiement > Déploiement avancé</td></tr><tr><td>Analyse > Utilisateurs > Sessions actives</td><td>est maintenu</td><td>Intégration > Utilisateurs > Sessions actives</td></tr><tr><td>Analyse > Utilisateurs > Utilisateurs</td><td>est maintenu</td><td>Intégration > Utilisateurs > Utilisateurs</td></tr><tr><td>Analyse > Utilisateurs > Activité de l'utilisateur</td><td>est maintenu</td><td>Intégration > Utilisateurs > Activité de l'utilisateur</td></tr></table>	Déployer > Historique de déploiement	est maintenu	Déployer > Historique de déploiement (🔍) (coin inférieur droit)	Déployer > Déploiement	est maintenu	Déploiement > Déploiement avancé	Analyse > Utilisateurs > Sessions actives	est maintenu	Intégration > Utilisateurs > Sessions actives	Analyse > Utilisateurs > Utilisateurs	est maintenu	Intégration > Utilisateurs > Utilisateurs	Analyse > Utilisateurs > Activité de l'utilisateur	est maintenu	Intégration > Utilisateurs > Activité de l'utilisateur
Déployer > Historique de déploiement	est maintenu	Déployer > Historique de déploiement (🔍) (coin inférieur droit)																
Déployer > Déploiement	est maintenu	Déploiement > Déploiement avancé																
Analyse > Utilisateurs > Sessions actives	est maintenu	Intégration > Utilisateurs > Sessions actives																
Analyse > Utilisateurs > Utilisateurs	est maintenu	Intégration > Utilisateurs > Utilisateurs																
Analyse > Utilisateurs > Activité de l'utilisateur	est maintenu	Intégration > Utilisateurs > Activité de l'utilisateur																
Dépannage																		
Statistiques des paquets abandonnés pour Secure Firewall 3100.	7.2.0	7.2.0	La nouvelle commande show packet-statistics Firewall Threat Defense affiche des informations complètes sur les abandons de paquets non liés à la politique. Auparavant, ces informations exigeaient l'utilisation de plusieurs commandes. Pour obtenir plus d'informations, reportez-vous à la Référence des commandes de défense contre les menaces de Cisco Secure Firewall.															
Fonctionnalités obsolètes																		

Caractéristiques	Version minimale Management Center	Défense minimale Version minimale de Threat Defense	Détails
Obsolète : EIGRP avec FlexConfig.	7.2.0	N'importe lequel	Vous pouvez maintenant configurer le routage EIGRP à partir de l'interface Web du On-Prem Firewall Management Center. Vous n'avez plus besoin des objets FlexConfig suivants : Eigrp_Configure, Eigrp_Interface_Configure, Eigrp_Unconfigure, Eigrp_Unconfigure_all. Et de ces objets textuels associés : eigrpAS, eigrpNetworks, eigrpDisableAutoSummary, eigrpRouterId, eigrpStubReceiveOnly, eigrpStubRedistributed, eigrpStubConnected, eigrpStubStatic, eigrpStubSummary, eigrpIntfList, eigrpAS, eigrpAuthKey, eigrpAuthKeyId, eigrpHelloInterval, eigrpHoldTime, eigrpDisableSplitHorizon. Le système vous permet d'effectuer un déploiement après la mise à niveau, mais vous avertit également de refaire vos configurations EIGRP. Pour vous aider dans ce processus, nous fournissons un outil de migration de ligne de commande. Pour en savoir plus, consultez Migration des politiques FlexConfig.
Obsolète : VXLAN avec FlexConfig.	7.2.0	N'importe lequel	Vous pouvez maintenant utiliser l'interface Web du On-Prem Firewall Management Center pour configurer les interfaces VXLAN. Vous n'avez plus besoin des objets FlexConfig suivants : VxLAN_Clear_Nve, VxLAN_Clear_Nve_Only, VxLAN_Configure_Port_And_Nve, VxLAN_Make_Nve_Only, VxLAN_Make_Vni. Et de ces objets texte associés : vxlan_Port_And_Nve, vxlan_Nve_Only, vxlan_Vni. Si vous avez configuré les interfaces VXLAN avec FlexConfig dans une version précédente, elles continuent de fonctionner. En fait, FlexConfig prévaut dans ce cas : si vous refaites vos configurations VXLAN dans l'interface Web, supprimez les paramètres FlexConfig.
Obsolète : dépannage automatique avant la mise à niveau.	7.2.0	N'importe lequel	Pour économiser du temps et de l'espace disque, le processus de mise à niveau du On-Prem Firewall Management Center ne génère plus automatiquement les fichiers de dépannage avant le début de la mise à niveau. Notez que les mises à niveau de périphériques ne sont pas affectées et continuent de générer des fichiers de dépannage. Pour générer manuellement des fichiers de dépannage pour le On-Prem Firewall Management Center, choisissez System (Système) (⚙️) > Health (Intégrité) > Monitor (Moniteur), cliquez sur Firewall Management Center dans le panneau de gauche, sur View System & Troubleshoot Details (Afficher les détails du système et du dépannage), puis sur Generate Troubleshooting Files (Générer les fichiers de résolution de problèmes).

Caractéristiques	Version minimale Management Center	Défense minimale Version minimale de Threat Defense	Détails
Obsolète : détails de géolocalisation	N'importe lequel	N'importe lequel	Nous ne fournissons plus le paquet IP de géolocalisation, qui contient des données contextuelles associées aux adresses IP routables. Cela permet d'économiser de l'espace disque et n'affecte en aucun cas les règles de géolocalisation ou la gestion du trafic. Toutes les données contextuelles sont maintenant obsolètes et la mise à niveau vers les versions ultérieures supprime le paquet IP. Les options permettant de télécharger le paquet IP ou d'afficher les données contextuelles n'ont aucun effet et sont supprimées dans les versions ultérieures.

Fonctionnalités Firewall Device Manager dans la version 7.2.x

Tableau 11 : Fonctionnalités Firewall Device Manager dans la version 7.2.x

Fonctionnalités	Description
Caractéristiques de la plateforme	
Firepower 1010E.	Nous avons lancé le périphérique Firepower 1010E, qui ne prend pas en charge l'alimentation par Ethernet (PoE). Version minimale de Threat Defense : 7.4.1 Voir Câblage du Firepower 1010
Threat Defense Virtual pour VMware sur VMware vSphere/VMware ESXi 8.0.	Vous pouvez maintenant déployer Threat Defense Virtual pour VMware sur VMware vSphere/VMware ESXi 8.0. Version minimale de Threat Defense : versions 7.2.9, 7.4.2 Voir : Guide de démarrage de Cisco Secure Firewall Threat Defense Virtual
Threat Defense Virtual pour GCP.	Vous pouvez maintenant utiliser le gestionnaire d'appareil pour configurer Threat Defense Virtual pour GCP. Voir : Guide de démarrage de Cisco Secure Firewall Threat Defense Virtual
Threat Defense Virtual pour Megaport.	Vous pouvez maintenant utiliser le gestionnaire d'appareil pour configurer Threat Defense Virtual pour Megaport (Megaport Virtual Edge). La haute disponibilité est prise en charge. Défense minimale contre les menaces : 7.2.8 Autres restrictions de version : au départ, vous ne pourrez peut-être pas déployer les versions 7.3.x ou 7.4.x. Déployez plutôt les versions 7.2.8–7.2.x et effectuez la mise à niveau. Voir : Guide de démarrage de Cisco Secure Firewall Threat Defense Virtual

Fonctionnalités	Description
Modules de réseau pour Cisco Secure Firewall 3100.	Nous avons présenté ces modules de réseau pour Cisco Secure Firewall 3130 : • Module de réseau à 6 ports 1G SFP, SX (multimode) (FPR-X-NM-6X1SX-F) • Module de réseau à 6 ports 10G SFP, SR (multimode) (FPR-X-NM-6X10SR-F) • Module de réseau à 6 ports 10G SFP, LR (mode unique) (FPR-X-NM-6X10LR-F) • Module de réseau à 6 ports 25G SFP, SR (multimode) (FPR-X-NM-X25SR-F) • Module de réseau à 6 ports 25G, LR (mode unique) (FPR-X-NM-6X25LR-F) • Module de réseau à 8 ports 1G, RJ45 (cuivre) (FPR-X-NM-8X1G-F) Version minimale de Threat Defense: 7.2.1
Pilote d'adaptateur de réseau Ethernet Intel E810-CQDA2 avec Threat Defense Virtual pour KVM.	Nous prenons désormais en charge le pilote d'adaptateur de réseau Ethernet Intel E810-CQDA2 avec Threat Defense Virtual pour KVM. Version minimale de Threat Defense: 7.2.1 Voir : Déployer Threat Defense Virtual sur KVM
Prise en charge d'ISA 3000 pour l'arrêt.	Demande de soutien concernant l'arrêt de l'ISA 3000. Cette fonctionnalité a été introduite dans la version 7.0.2, mais a été temporairement obsolète dans la version 7.1.
Fonctionnalités de pare-feu et IPS	
La recherche de groupe d'objets est activée par défaut pour le contrôle d'accès.	La commande de configuration de la CLI object-group-search access-control est maintenant activée par défaut pour les nouveaux déploiements. Toutefois, si vous effectuez une mise à niveau vers la version 7.2, le paramètre reste activé ou désactivé en fonction de vos paramètres précédents. Si vous configurez la commande à l'aide de FlexConfig, vous devez évaluer si cela est toujours nécessaire. Si vous devez désactiver la fonctionnalité, utilisez FlexConfig pour mettre en œuvre la commande no object-group-search access-control. Voir : Référence des commandes de la série Cisco Secure Firewall ASA
Le nombre de règles persiste pendant le redémarrage.	Le redémarrage d'un périphérique ne réinitialise plus le nombre de résultats de règles de contrôle d'accès à zéro. Le nombre de résultats est réinitialisé uniquement si vous effacez activement les compteurs. En outre, les décomptes sont gérés séparément par chaque unité d'une paire ou d'une grappe à haute disponibilité. Vous pouvez utiliser la commande show rule hits pour afficher les compteurs cumulés pour la paire ou la grappe à haute disponibilité, ou pour voir le nombre par nœud. Nous avons modifié Cisco Firewall Threat Defense la commande CLI suivante: show rule hits. Voir : Examiner le nombre de résultats pour les règles
Fonctionnalités du VPN	

Fonctionnalités	Description
Décharge de flux IPsec.	Sur la Secure Firewall 3100, les flux IPsec sont déchargés par défaut. Après la configuration initiale d'une association de sécurité (SA), d'un VPN de site à site ou d'un VPN d'accès à distance IPsec, les connexions IPsec sont déchargées vers le FPGA (field programmable gate RAID) dans le périphérique, ce qui devrait améliorer les performances du périphérique. Vous pouvez modifier la configuration à l'aide de FlexConfig et de la commande flow-offload-ipsec. Voir : Décharge de flux IPSec
Fonctionnalités de l'interface	
Prise en charge des ports d'éclatement pour Cisco Secure Firewall 3130 et 3140.	Vous pouvez maintenant configurer quatre ports d'éclatement de 10 Go pour chaque interface de 40 Go sur les Cisco Secure Firewall 3130 et 3140. Écrans nouveaux ou modifiés : Device (périphérique) > Interfaces Voir : Gérer le module de réseau pour Cisco Secure Firewall 3100
Activation ou désactivation de Cisco Trustsec sur une interface.	Vous pouvez activer ou désactiver Cisco Trustsec sur les interfaces physiques, les sous-interfaces, les interfaces EtherChannel, VLAN, les interfaces de gestion ou BVI, qu'elles soient nommées ou non. Par défaut, Cisco Trustsec est activé automatiquement lorsque vous nommez une interface. Nous avons ajouté l'attribut Propagate Security Group Tag (propager la balise de groupe de sécurité) aux boîtes de dialogue de configuration d'interface et l'attribut ctsEnabled aux différentes API d'interface. Voir : Configurer les options avancées
Caractéristiques de la licence	
Prise en charge de la réservation de licence permanente pour ISA 3000.	ISA 3000 prend désormais en charge la réservation de licences permanentes universelles pour les clients approuvés. Voir : Application des licences permanentes dans les réseaux isolés
Fonctions d'administration et de dépannage	
Capacité de forcer le déploiement complet.	Lorsque vous déployez des modifications, le système déploie normalement les modifications apportées depuis le dernier déploiement réussi. Toutefois, si vous rencontrez des problèmes, vous pouvez choisir de forcer un déploiement complet, ce qui actualise complètement la configuration sur le périphérique. Nous avons ajouté l'option Apply Full Deployment (appliquer le déploiement complet) à la boîte de dialogue de déploiement. Voir : Déployer vos modifications

Fonctionnalités	Description
Mettre automatiquement à jour les ensembles d'autorités de certification.	Incidence sur la mise à niveau. Le système se connecte à Cisco dans le cadre d'une nouveauté. L'offre groupée de l'autorité de certification locale contient des certificats pour accéder à plusieurs services Cisco. Le système interroge désormais automatiquement Cisco pour obtenir de nouveaux certificats d'autorité de certification à une heure quotidienne définie par le système. Auparavant, vous deviez mettre à niveau le logiciel pour mettre à jour les certificats d'autorité de certification. Vous pouvez utiliser l'interface de ligne de commande pour désactiver cette fonctionnalité. Nouvelles ressources : https://cisco.com/security/pki/ Commandes CLI nouvelles ou modifiées : configure cert-update auto-update, configure cert-update run-now, configure cert-update test, show cert-update Restrictions de version : nécessite la version 7.0.5, 7.1.0.3 ou 7.2.4. Non pris en charge avec les versions 7.0.0 à 7.0.4, 7.1.0 à 7.1.0.2 ou 7.2.0 à 7.2.3. Voir : Référence des commandes de défense contre les menaces de Cisco Secure Firewall
Exiger l'attribut Message-Authenticator dans toutes les réponses RADIUS.	Incidence sur la mise à niveau. Après la mise à niveau, lancez l'activation pour les serveurs existants. Vous pouvez désormais exiger l'attribut Message-Authenticator dans toutes les réponses RADIUS, en vous assurant que la passerelle VPN de défense contre les menaces vérifie de manière sécurisée chaque réponse du serveur RADIUS, qu'il s'agisse d'un VPN d'accès à distance ou de l'accès au périphérique lui-même. L'option Require Message-Authenticator for all RADIUS Responses (exiger l'authentificateur Message-Authenticator pour toutes les réponses envoyées par RADIUS) est activée par défaut pour les nouveaux serveurs RADIUS. Nous vous recommandons également de l'activer pour les serveurs existants. Sa désactivation peut exposer les pare-feu à des attaques potentielles. Nouvelles commandes CLI : message-authenticator-required Restrictions de version : nécessite la version 7.0.7/7.2.10/ 7.7.0 (ou version ultérieure).
API REST Threat Defense, version 6.3 (v6).	L'API REST Cisco Firewall Threat Defense pour la version logicielle 7.2 est la version 6.3. Vous pouvez utiliser la version v6 dans les URL d'API ou, de préférence, utiliser /latest/ pour signifier que vous utilisez la version d'API la plus récente prise en charge sur le périphérique. Notez que l'élément de chemin de version d'URL pour la version 6.3 est le même que pour les versions 6.0, 6.1 et 6.2 : v6. Veillez réévaluer tous les appels existants, car des modifications peuvent avoir été apportées aux modèles de ressources que vous utilisez. Pour ouvrir l'API Explorer et consulter les ressources, connectez-vous à Firepower Device Manager, cliquez sur le bouton Plus d'options (⋮) et choisissez API Explorer. Voir : Guide de Cisco Secure Firewall Threat Defense REST API

Fonctionnalités et incidence de la mise à niveau

Une fonctionnalité a une incidence sur la mise à niveau si sa mise à niveau et son déploiement peuvent forcer le système à traiter le trafic ou à agir différemment sans autre action de votre part. Cela arrive fréquemment avec les nouvelles capacités de détection des menaces et d'identification des applications. Une fonctionnalité peut également avoir une incidence sur la mise à niveau si celle-ci implique que vous preniez des mesures avant ou après la mise à niveau pour éviter un résultat indésirable; par exemple, si vous devez modifier une configuration.



Important

Minimisez l'incidence de la mise à niveau et autres en accédant directement à la dernière version de maintenance de la version choisie. Consultez [Choix de votre cible de mise à niveau, à la page 51](#).

Fonctionnalités et incidence de la mise à niveau pour On-Prem Firewall Management Center

Tableau 12 : Fonctionnalités et incidence de la mise à niveau pour On-Prem Firewall Management Center

Version cible	Fonctionnalités ayant une incidence sur la mise à niveau
7.2.10–7.2.x	• Nouvelle méthode de connexion en nuage Cisco Advanced Malware Protection. • Mise à jour des exigences d'accès Internet pour les licences Smart.
7.2.6–7.2.x	• Configurez les interfaces de confiance de relais DHCP à partir de l'interface Web du On-Prem Firewall Management Center. • Mise à jour des exigences d'accès Internet pour le téléchargement direct des mises à niveau logicielles. • Obsolète : téléchargement programmé des versions de maintenance. • Mise à jour du fournisseur de services d'analyse web.
7.2.5–7.2.x	• Le centre de gestion détecte les erreurs de synchronisation d'interface.
7.2.4–7.2.x	• VDB de taille plus restreinte pour les périphériques Snort 2 à faible mémoire. • Mettre automatiquement à jour les ensembles d'autorités de certification.
7.2.4 à 7.2.5	• Améliorations de la performance du contrôle d'accès (optimisation des objets).
7.2.0+	• Configurez VXLAN à partir de l'interface Web du On-Prem Firewall Management Center. • Configurer le protocole EIGRP à partir de l'interface Web du On-Prem Firewall Management Center.

Version cible	Fonctionnalités ayant une incidence sur la mise à niveau
7.1.0+	• Configurez les chemins multiples à coûts égaux (Equal-Cost-Multi-path (ECMP)) à partir de l'interface Web de FMC. • Configurez le routage basé sur les politiques à partir de l'interface Web de FMC. • Envoyez des incidents d'intrusion et des événements rétrospectifs de programmes malveillants au nuage Cisco Secure Network Analytics à partir de FMC. • Obsolète (temporaire) : Intégration SecureX et orchestration SecureX améliorées. • Obsolète : incidents des intrusions et presse-papiers des incidents d'intrusion. • Obsolète : tableaux personnalisés pour les incidents d'intrusion.
6.7.0 et les versions ultérieures	• Fin de prise en charge : VMware vSphere/VMware ESXi 6.0. • Obsolète : communications sur le port 3237 avec les nuages AMP.
6.7.0 et les versions ultérieures	• Modifications apportées à l'attribution d'adresses PAT dans la mise en grappe. • pxGrid 2.0 avec ISE/ISE-PIC. • L'amélioration de la préclassification des fichiers pour l'analyse dynamique. • La base de données nationale sur les vulnérabilités (NVD) remplace Bugtraq. • Vérification de compatibilité préalable à la mise à niveau. • Les mises à niveau reportent les tâches planifiées. • Les mises à niveau suppriment les fichiers PCAP pour économiser de l'espace disque. • Obsolète : logiciel d'agent d'utilisateur Cisco Firepower et source d'identité. • Obsolète : mesure corrective de Cisco ISE EPS (Endpoint Protection Services, service de protection des terminaux). • Obsolète : groupes Diffie-Hellman, algorithmes de chiffrement et de hachage moins sécurisés. • Obsolète : module d'intégrité Utilisation des ressources de configuration de l'appareil (temporaire).

Fonctionnalités et incidence de la mise à niveau pour Firewall Threat Defense avec On-Prem Firewall Management Center

Tableau 13 : Fonctionnalités et incidence de la mise à niveau pour Firewall Threat Defense avec On-Prem Firewall Management Center

Version actuelle	Fonctionnalités ayant une incidence sur la mise à niveau
7.2.0–7.2.9 7.1.x 7.0.6 et versions antérieures	Exiger l'attribut Message-Authenticator dans toutes les réponses RADIUS. (7.0.7)
7.2.9 et versions antérieures	Gestion du trafic asymétrique. (7.2.9)
7.2.0–7.2.3 7.1.0–7.1.0.2 7.0.4 et versions antérieures	Mettre automatiquement à jour les ensembles d'autorités de certification. (7.0.5)
7.1.x et versions antérieures	Mise à l'échelle automatique pour Firewall Threat Defense Virtual pour GCP. (7.2.0)
7.0.x et versions antérieures	- Prise en charge de Snort 3 pour l'inspection de DCE/RPC sur SMB2. (7.1.0) - Prise en charge de Snort 3 pour les mots-clés <code>ssl_version</code> et <code>ssl_state</code>. (7.1.0)
6.7.x et versions antérieures	- Fin de prise en charge : VMware vSphere/VMware ESXi 6.0. (7.0.0) - Niveaux de performance pour les licences Smart de FTDv (7.0.0) - Obsolète : Certificats RSA dont les clés sont inférieures à 2 048 bits ou qui utilisent SHA-1 dans leur algorithme de signature. (7.0.0) - Obsolète : algorithme d'authentification MD5 et chiffrement DES pour les utilisateurs SNMPv3. (7.0.0)
6.6.x et versions antérieures	- Les interfaces SFP des séries Firepower 1100/2100 prennent désormais en charge la désactivation de la négociation automatique. (6.7.0) - Modification de ClientHello pour les règles TLS/SSL de l'action Déchiffrer - Clé connue. (6.7.0) - Vérification de compatibilité préalable à la mise à niveau. (6.7.0) - Améliorations des vérifications de l'état de préparation. (6.7.0) - Amélioration des rapports sur l'état de la mise à niveau de FTD et des options d'annulation et de nouvelle tentative. (6.7.0) - Les mises à niveau suppriment les fichiers PCAP pour économiser de l'espace disque. (6.7.0)

Fonctionnalités et incidence de la mise à niveau pour Firewall Threat Defense avec Firepower Device Manager

Tableau 14 : Fonctionnalités et incidence de la mise à niveau pour Firewall Threat Defense avec Firepower Device Manager

Version cible	Caractéristiques
7.2.10–7.2.x	Exiger l'attribut Message-Authenticator dans toutes les réponses RADIUS.
7.2.4–7.2.x	Mettre automatiquement à jour les ensembles d'autorités de certification.
7.1.0+	- Prise en charge du système de nom de domaine dynamique (DDNS) pour la mise à jour du nom de domaine complet (FQDN) aux mappages d'adresses IP pour les interfaces du système. - Prise en charge de Snort 3 pour l'inspection de DCE/RPC sur SMB2. - Prise en charge de Snort 3 pour les mots-clés <code>ssl_version</code> et <code>ssl_state</code>.
7.0.0 et les versions ultérieures	- Fin de prise en charge : VMware vSphere/VMware ESXi 6.0. - Configuration du relais DHCP à l'aide de l'API Cisco Firewall Threat Defense.
6.7.0 et les versions ultérieures	- Suppression de la prise en charge des groupes Diffie-Hellman moins sécurisés, et des algorithmes de chiffrement et de hachage. - Prise en charge du protocole EIGRP à l'aide de Smart CLI. - Prise en charge de l'API Firewall Threat Defense pour la configuration de SNMP.

Directives de mise à niveau

Les sections suivantes contiennent des avertissements et des lignes directrices de mise à niveau spécifiques à la version. Vous devez également vérifier les fonctionnalités et les bogues ayant une incidence sur la mise à niveau. Pour obtenir des renseignements généraux sur les exigences de temps/espace disque et sur le comportement du système pendant la mise à niveau, qui peut inclure des interruptions du flux de trafic et de l'inspection, consultez le guide de mise à niveau approprié : [Pour de l'assistance, à la page 191](#).

Directives de mise à niveau pour On-Prem Firewall Management Center

Tableau 15 : Directives de mise à niveau pour On-Prem Firewall Management Center

Version actuelle	Directives	Détails
7.2.8.x	Désinstallation de correctif non prise en charge : de la version 7.2.8.x à la version 7.2.8.0.	La désinstallation n'est pas prise en charge pour le correctif du centre de gestion en version 7.2.8.1. Comme les correctifs sont cumulés et que la désinstallation vous ramène au niveau de correctif à partir duquel vous avez effectué la mise à niveau, cela signifie que la désinstallation n'est pas prise en charge à partir d'un correctif de la version 7.2.8.x à la version 7.2.8 (la version de base).

Version actuelle	Directives	Détails
N'importe lequel	Mise à niveau non conseillée : version 7.2.6.	Suite au bogue CSCwi63113 , la version 7.2.6 a été reportée le 29-04-2024 et n'est plus téléchargeable. Si vous l'avez téléchargée, ne l'utilisez pas. Si vous utilisez cette version, effectuez la mise à niveau.
6.4.0–6.7.x	Reconnecter avec Cisco Threat Grid pour les centres de gestion à haute disponibilité.	La version 7.0.0 corrige un problème de haute disponibilité du centre de gestion et de détection des programmes malveillants où, après un basculement, le système cessait de soumettre des fichiers pour analyse dynamique (CSCvu35704). Pour que le correctif prenne effet, vous devez vous réassocier au nuage public Cisco Threat Grid après la mise à niveau. Après avoir mis à niveau la paire à haute disponibilité vers la version 7.0.0+, sur le centre de gestion principal : 1. Choisissez AMP > Connexions d'analyse dynamique. 2. Cliquez sur Associer dans la ligne du tableau correspondant au nuage public. Une fenêtre de portail s'ouvre. Vous n'avez pas besoin de vous connecter. La réassociation se produit en arrière-plan, en quelques minutes.

Directives de mise à niveau pour Firewall Threat Defense avec On-Prem Firewall Management Center

Tableau 16 : Directives de mise à niveau pour Firewall Threat Defense

Version actuelle	Directives	Détails
N'importe lequel	Mise à niveau non conseillée : version 7.2.6.	Suite au bogue CSCwi63113 , la version 7.2.6 a été reportée le 29-04-2024 et n'est plus téléchargeable. Si vous l'avez téléchargée, ne l'utilisez pas. Si vous utilisez cette version, effectuez la mise à niveau.
6.6 et antérieure	Échec de la mise à niveau : ports de commutation du Firepower 1010 avec des identifiants VLAN non valides	Pour le Firepower 1010, les mises à niveau de vers la version 6.7 ou une version ultérieure échoueront si vous avez configuré des ports de commutation avec un identifiant de VLAN compris entre 3968 et 4047. Switch "Firewall Threat Defense and "Ces identifiants sont destinés à un usage interne uniquement Ces identifiants sont destinés à un usage interne uniquement

Directives de mise à niveau pour Firewall Threat Defense avec Firepower Device Manager

Tableau 17 : Directives de mise à niveau pour Firewall Threat Defense

Version actuelle	Directives	Détails
N'importe lequel	Mise à niveau non conseillée : version 7.2.6.	Suite au bogue CSCwi63113 , la version 7.2.6 a été reportée le 29-04-2024 et n'est plus téléchargeable. Si vous l'avez téléchargée, ne l'utilisez pas. Si vous utilisez cette version, effectuez la mise à niveau.

Version actuelle	Directives	Détails
6.6 et antérieure	Échec de la mise à niveau : ports de commutation du Firepower 1010 avec des identifiants VLAN non valides	Pour le Firepower 1010, les mises à niveau de vers la version 6.7 ou une version ultérieure échoueront si vous avez configuré des ports de commutation avec un identifiant de VLAN compris entre 3968 et 4047. Switch "Firewall Threat Defense and "Ces identifiants sont destinés à un usage interne uniquement Ces identifiants sont destinés à un usage interne uniquement

Directives de mise à niveau pour le châssis Firepower 4100/9300

Dans la plupart des cas, nous vous recommandons d'utiliser la dernière version de FXOS dans chaque version principale.

Pour les avertissements et les directives de mise à niveau de FXOS spécifiques à la version, ainsi que les fonctionnalités et les bogues ayant une incidence sur la mise à niveau, consultez toutes les notes de mise à jour entre votre version actuelle et la version cible : <http://www.cisco.com/go/firepower9300-rns>.

Pour obtenir des directives sur la mise à niveau de micrologiciel (pour les mises à niveau vers FXOS 2.13 et versions antérieures), consultez le guide de mise à niveau de micrologiciel : [CGuide de mise à niveau du micrologiciel Cisco Firepower 4100/9300 FXOS](#).

Chemin de mise à niveau

La planification de votre chemin et de votre ordre de mise à niveau est particulièrement importante pour les déploiements importants, la haute disponibilité/mise en grappe, les mises à niveau multisauts et les situations où vous devez coordonner des châssis, des environnements d'hébergement ou d'autres mises à niveau. Ces scénarios, ainsi que les renseignements sur la restauration et la désinstallation, sont traités plus en détail dans le guide de mise à niveau : [Pour de l'assistance, à la page 191](#).

Choix de votre cible de mise à niveau

Accédez **directement à la dernière** version de maintenance pour minimiser l'incidence de la mise à niveau et autres.

En effet, les fonctionnalités, les améliorations et les correctifs critiques peuvent ignorer les versions « futures » qui sont à venir par version, mais pas par date de version. Par exemple, si vous êtes à jour dans la version majeure A, la mise à niveau vers la version B à point zéro peut rendre les fonctionnalités et les correctifs obsolètes.

Si vous ne pouvez pas accéder à la dernière version, assurez-vous au moins que votre version actuelle a été publiée à une date antérieure à celle de votre version cible. Dans le tableau suivant, vérifiez que votre version actuelle figure à côté de votre version cible. Si ce n'est pas le cas, choisissez une cible ultérieure.

Tableau 18 : Version antérieure à la version 7.2.x, par date

Version cible		Version actuelle : vérifiez que la vôtre figure dans la liste.				
		depuis 6.6	6.7	7.0	7.1	7.2
vers 7.2.10	2025-05-22	6.6.0–6.6.7	6.7.0	7.0.0–7.0.7	7.1.0	7.2.0–7.2.9

Version cible		Version actuelle : vérifiez que la vôtre figure dans la liste.				
		depuis 6.6	6.7	7.0	7.1	7.2
vers 7.2.9	2024-10-22	6.6.0–6.6.7	6.7.0	7.0.0–7.0.6	7.1.0	7.2.0–7.2.8
vers 7.2.8	2024-06-24	6.6.0–6.6.7	6.7.0	7.0.0–7.0.6	7.1.0	7.2.0–7.2.7
vers 7.2.7	2024-04-29	6.6.0–6.6.7	6.7.0	7.0.0–7.0.6	7.1.0	7.2.0–7.2.6
vers 7.2.6*	2024-03-19	—	—	—	—	—
vers 7.2.5	2023-07-27	6.6.0–6.6.7	6.7.0	7.0.0–7.0.6	7.1.0	7.2.0–7.2.4
vers 7.2.4	2023-05-03	6.6.0–6.6.7	6.7.0	7.0.0–7.0.5	7.1.0	7.2.0–7.2.3
vers 7.2.3	2023-02-27	6.6.0–6.6.7	6.7.0	7.0.0–7.0.5	7.1.0	7.2.0–7.2.2
vers 7.2.2	2022-11-29	6.6.0–6.6.7	6.7.0	7.0.0–7.0.5	7.1.0	7.2.0–7.2.1
vers 7.2.1	2022-10-03	6.6.0–6.6.7	6.7.0	7.0.0–7.0.4	7.1.0	7.2.0
vers 7.2.0	2022-06-06	6.6.0–6.6.5	6.7.0	7.0.0–7.0.2	7.1.0	—

* La version 7.2.6 n'est plus disponible.

Mise à niveau à partir d'un déploiement corrigé

Les correctifs critiques dans les versions de correctifs (quatrième chiffre) peuvent également ignorer les versions futures. Si vous dépendez de ces correctifs critiques, vérifiez que votre version cible les contient. Pour obtenir une liste complète des dates de version, consultez [Nouvelles fonctionnalités de Cisco Secure Firewall Management Center par version](#) ou [Nouvelles fonctionnalités de Cisco Secure Firewall Device Manager par version](#).

Mises à niveau et rétrogradations prises en charge

Cette section résume les capacités de mise à niveau et de rétrogradation. Pour obtenir de l'aide pour :

- Choisir une cible de mise à niveau, consultez [Choix de votre cible de mise à niveau, à la page 51](#).
- Les procédures de mise à niveau et de rétrogradation, y compris les directives générales, les bonnes pratiques et le dépannage, consultez le guide de mise à niveau pour la version que vous utilisez actuellement : <https://www.cisco.com/go/ftd-upgrade>.

Mises à niveau prises en charge

Ce tableau présente les mises à niveau directes prises en charge pour On-Prem Firewall Management Center et le logiciel Firewall Threat Defense Threat Defense.

**Remarque**

Vous pouvez effectuer directement une mise à niveau vers les versions majeures (premier et deuxième chiffres) ou de maintenance (troisième chiffre). Les correctifs modifient uniquement le quatrième chiffre. Vous ne pouvez pas effectuer de mise à niveau directement vers un correctif à partir d'une version majeure ou d'une version de maintenance précédente. Bien qu'un périphérique corrigé (quatre chiffres) puisse être géré avec un On-Prem Firewall Management Center non corrigé, les déploiements entièrement corrigés sont soumis à des tests avancés.

Pour les périphériques Firepower 4100/9300, le tableau répertorie également les versions FXOS associées. Si une mise à niveau de châssis est requise, la mise à niveau de Firewall Threat Defense est bloquée. Dans la plupart des cas, nous recommandons la dernière version de chaque version; pour les versions minimales, consultez le [Guide de compatibilité de Cisco Secure Firewall Threat Defense](#).

Tableau 19 : Mises à niveau directes prises en charge

Version actuelle	Version du logiciel cible						
	vers 7.7	7.6	7.4*	7.3	7.2	7.1	7.0
	Version FXOS pour les mises à niveau du châssis Firepower 4100/9300						
	vers 2.17	2.16	2.14	2.13	2.12	2.11	2.10
depuis 7.7	OUI	—	—	—	—	—	—
depuis 7.6	OUI	OUI	—	—	—	—	—
depuis 7.4	OUI	OUI	OUI	—	—	—	—
de 7.3	OUI	OUI	OUI	OUI	—	—	—
depuis 7.2	OUI	OUI	OUI	OUI	OUI	—	—
depuis 7.1	—	OUI	OUI	OUI	OUI	OUI	—
depuis 7.0	—	—	OUI	OUI	OUI	OUI	OUI
depuis 6.4	—	—	—	—	—	—	OUI

* Vous ne pouvez pas mettre à niveau Firewall Threat Defense vers la version 7.4.0, qui est disponible en tant que nouvelle installation sur Secure Firewall 4200 uniquement, et n'est pas pris en charge avec Firepower Device Manager. Elle supprime des fonctionnalités, des améliorations et des correctifs critiques inclus dans les versions précédentes. Effectuez une mise à niveau vers une version ultérieure.

Rétrogradations prises en charge

Si une mise à niveau ou un correctif réussit, mais que le système ne fonctionne pas comme prévu, vous pouvez annuler (Firewall Threat Defense mises à niveau) ou désinstaller (Firewall Threat Defense et On-Prem Firewall Management Center correctifs). Pour obtenir des renseignements généraux, en particulier sur les scénarios courants dans lesquels le retour à une version précédente n'est pas pris en charge ou conseillé, consultez le guide de mise à niveau : <https://cisco.com/go/ftd-upgrade>.

Bogues

Pour les bogues des versions antérieures, consultez les notes de mise à jour de ces versions. Pour les déploiements dans le nuage, consultez le [Notes de mise à jour de Cisco Firewall Management Center en nuage](#).



Important Nous ne répertorions pas les bogues ouverts de la des versions de maintenance ou des correctifs.



Important Les listes de bogues sont générées automatiquement une fois et peuvent ne pas être mises à jour par la suite. Si elle est mise à jour, la date de la « dernière mise à jour du tableau » ne signifie pas que la liste était entièrement précise à cette date; seulement que des modifications ont été apportées. Selon la façon et le moment où un bogue a été classé ou mis à jour dans notre système, il se peut qu'il ne s'affiche pas dans les notes de mise à jour. Si vous disposez d'un contrat d'assistance, vous pouvez utiliser l'[outil de recherche de bogues](#) pour obtenir des listes de bogues à jour.

Bogues ouverts dans la version 7.2.0

Dernière mise à jour du tableau : 02-05-2024

Tableau 20 : Bogues ouverts dans la version 7.2.0

ID du bogue	En-tête :
CSCwb43433	Les performances des trames jumbo ont diminué jusqu'à -45 % sur la série Firepower 2100
CSCwb78233	7.2.0 1984 Nutanix vFMC n'est pas accessible après la mise à niveau à partir de la version 7.1.0
CSCwb80789	Les connexions TLS 1.3 aux sites précédemment déchiffrés peuvent échouer
CSCwb87724	Les unités expulsées ont rejoint la grappe existante, mais ne figurent pas dans la grappe de contrôle et d'autres grappes vFTD expulsées
CSCwb88887	snp_fp_vxlan_encap_and_grp_send_common : échec de recherche d'adj. bp->l3_type = 8, message inner_sip
CSCwb89905	vFTD installé avec JF, mais FMC affiche toujours des informations sur l'activation de JF et pour redémarrer vFTD
CSCwb90105	La mise à niveau vers la version 7.2 sur FTDv pour Nutanix est bloquée après le redémarrage
CSCwb96990	Les données précoces peuvent faire en sorte que les xtls n'attendent pas la réponse de la sonde
CSCwb97486	FPR3100 : les ports à fibre optique 25 G peuvent afficher une liaison sur certains ports à fibre optique uniquement compatibles avec le 1/10G
CSCwb99960	onPremFMC avec uniquement des périphériques gérés par CDO enregistrés, les pages d'événements de programmes malveillants affichent un avertissement de licence

ID du bogue	En-tête :
CSCwd07838	L'utilisateur ne peut pas filtrer par périphérique dans la nouvelle interface utilisateur de politique AC
CSCwd16602	Incohérences observées après le passage de l'ancienne interface utilisateur à la nouvelle interface utilisateur sans enregistrer la politique
CSCwd47149	Nouvelle interface utilisateur de politique AC : La liste des règles ACP prend du temps à se charger dans le cas d'un ensemble de règles volumineux
CSCwe14714	La recherche est lente et les recherches sémantiques ne fonctionnent pas dans la nouvelle interface utilisateur d'ACP
CSCwe96560	Impossible de copier les règles d'une politique vers une autre politique en utilisant la nouvelle interface utilisateur de politique AC
CSCwh15444	La récupération du nombre de résultats prend plus de temps dans la nouvelle interface utilisateur de ACP que dans l'ancienne interface utilisateur de ACP
CSCwi22693	La règle ACP est supprimée lors de la suppression des modifications après le repositionnement de la règle.

Bogues résolus dans la version 7.2.10.2

Dernière mise à jour du tableau : 25-09-2025

Tableau 21 : Bogues de sécurité résolus dans la version 7.2.10.2

ID du bogue	En-tête :
CSCwq79815	Vulnérabilité d'accès non autorisé au serveur Web VPN du logiciel Cisco Secure Firewall Adaptive Security Appliance et du logiciel Cisco Secure Firewall Threat Defense
CSCwq79831	Vulnérabilité d'exécution de code à distance sur le serveur Web VPN du logiciel Cisco Secure Firewall Adaptive Security Appliance et du logiciel Cisco Secure Firewall Threat Defense

Bogues résolus dans la version 7.2.10.1

Dernière mise à jour du tableau : 13/10/2025

Tableau 22 : Bogues de sécurité résolus dans la version 7.2.10.1

ID du bogue	En-tête :
CSCwq03404	Connexion authentifiée externe avec RADIUS à l'interface utilisateur de FMC peut échouer si l'attribut de classe est utilisé
CSCwq10344	Demandes d'accès par authentification extérieure RADIUS pour FMC manquantes 6 attributs après la mise à niveau de FMC

Dernière mise à jour du tableau : 13-10-2025

Tableau 23 : Bogues fonctionnels résolus dans la version 7.2.10.1

ID du bogue	En-tête :
CSCwj68277	L'enregistrement du certificat dans les paramètres LDAP est trop restrictif
CSCwo71835	L'attribut NAS-IP-Address est manquant dans la demande d'accès dans FMC
CSCwq46783	L'authentification FMC échoue avec l'erreur freeradius, « Invalid NAS IP Address » (adresse IP invalide de la NAS) affiche une adresse IP inattendue
CSCwq86675	Le nombre de sessions en cache pour Tomcat est défini incorrectement
CSCwq92436	L'attribut de l'identifiant NAS a toujours la valeur « sshd »

Bogues résolus dans la version 7.2.10

Dernière mise à jour du tableau : 22/05/2025

Tableau 24 : Bogues de sécurité résolus dans la version 7.2.10

ID du bogue	En-tête :
CSCwe86964	Consul et Consul Enterprise ont autorisé un utilisateur authentifié avec le service :
CSCwh20307	Échec du déploiement de FMC après le retrait de la règle de NAT ou d'ACL
CSCwi46163	Vulnérabilité de validation d'entrée incorrecte dans Apache Tomcat à partir de la version 11.
CSCwi64429	L'utilisation de la mémoire MonetDB augmente lentement au fil du temps
CSCwi65260	Échec de la modification des entrées de destination, lorsque SOG et DOG contiennent le même groupe d'objets internes
CSCwj33734	La bibliothèque d'interfaces graphiques de réseau portables (libpng) 1.0.15 et versions antérieures permet
CSCwj79229	FMC : mots de passe en texte brut pour le profil d'authentification extérieure « Radius Server Key » (clé du serveur RADIUS)
CSCwj89126	Fractionnement de la réponse HTTP en plusieurs modules dans le serveur HTTP Apache permet
CSCwk05564	Seule la région des États-Unis dans les services en nuage de FDM.
CSCwk21540	Impossible d'établir la session RAVPN sur la configuration de FTD à haute disponibilité
CSCwk66255	urllib3 est une bibliothèque cliente HTTP conviviale pour Python. Lors de l'utilisation de
CSCwk67859	FTD et FXOS : Vulnérabilité d'usurpation de protocole RADIUS (Blast-RADIUS) : 07/2024

ID du bogue	En-tête :
CSCwk67902	FTD : Vulnérabilité d'usurpation de protocole RADIUS (Blast-RADIUS) : 07/2024
CSCwk69454	FDM : Blast-RADIUS CVE-2024-3596
CSCwk71817	FMC : Blast-RADIUS CVE-2024-3596
CSCwk72477	Règle personnalisée avec « metadata:impact_flag rouge » dans Snort3 non détectée en tant que Niveau d'impact 1
CSCwk74997	Avec CVE-ID, impossible de rechercher les événements IPS sur le FMC
CSCwk75832	Rechargements Snort3 lorsque le rechargement d'AppID et les redémarrages de Snort se produisent simultanément
CSCwk93503	environ 400 tâches ont été créées sur le FMC principal pour installer les mises à jour de VDB sur le FMC en veille
CSCwm12775	Dans le noyau Linux, la vulnérabilité suivante a été résolue : c
CSCwm12882	Validation de certificat incorrecte dans Node.js 10, 12 et 13 entraîne le p
CSCwm12884	Contrebande de requêtes HTTP dans Node.js 10, 12 et 13 entraîne des charges utiles malveillantes
CSCwm12885	Inclusion d'espaces blancs de fin dans les valeurs d'en-tête HTTP dans Node.js 10, 12,
CSCwm12896	Les versions de Node.js antérieures à 10.23.1, 12.20.1, 14.15.4 et 15.5.1 sont vulnérables
CSCwm12897	Les versions de Node.js antérieures à 10.23.1, 12.20.1, 14.15.4 et 15.5.1 permettent deux co
CSCwm12898	Node.js avant les versions 10.24.0, 12.21.0, 14.16.0 et 15.10.0 est vulnérable à
CSCwm12901	Node.js avant les versions 10.24.0, 12.21.0, 14.16.0 et 15.10.0 est vulnérable à
CSCwm12902	Acceptation de types arbitraires de nom alternatif du sujet (SAN), sauf si un PKI
CSCwm12905	Node.js < 12.22.9, < 14.18.3, < 16.13.2 et < 17.3.1 convertit les SAN (S
CSCwm12907	Node.js < 12.22.9, < 14.18.3, < 16.13.2 et < 17.3.1 n'a pas géré m
CSCwm29876	Problème d'encodage de substitution dans mod_rewrite dans le serveur HTTP Apache 2.4.5
CSCwm29879	Vulnérabilité suivante résolue dans le noyau Linux : b
CSCwm43165	Vulnérabilité suivante résolue dans le noyau Linux : n
CSCwm43186	Vulnérabilité suivante résolue dans le noyau Linux : x
CSCwm43304	Vulnérabilité suivante résolue dans le noyau Linux : p
CSCwm44719	Recherche de la source FTD Snort3 dans daq_pkt_msg

ID du bogue	En-tête :
CSCwm49410	Cross-Origin-Opener-Policy mal configuré
CSCwm50895	Onglet ou espace supplémentaire ajouté dans les messages de journalisation d'ACL au format EMBLEM, ce qui provoque des problèmes d'intégration
CSCwm56972	Vulnérabilité suivante résolue dans le noyau Linux : x
CSCwm57062	Dans le noyau Linux, pour usb : xhci : vérifier que le point terminal est valide avant de le déréférencer
CSCwm57472	Dans le noyau Linux, pour filelock : retrait des verrous de manière fiable lorsque fcntl/fermer la concurrence est détecté
CSCwm57484	Dans le noyau Linux, en mm : éviter les débordements dans la logique de régulation des écritures
CSCwm75514	Faible trouvée dans le paquet python-cryptography. Ce problème peut également
CSCwm75547	Vulnérabilité suivante résolue dans le noyau Linux : b
CSCwm75696	Dans le noyau Linux, pour dma : correctif de l'ordre d'appel dans dmam_free_coherent dmam_free_coherent()
CSCwm75710	Correction d'une erreur de vérification des autorisations d'accès aux fichiers du noyau Linux
CSCwm75719	Correction d'une erreur de division du noyau Linux par zéro lors de l'appel de ioctl TIOCSSERIAL avec un mauvais débit (en bauds)
CSCwm87845	Vulnérabilité suivante résolue dans le noyau Linux : m
CSCwm87847	Vulnérabilité suivante résolue dans le noyau Linux : g
CSCwm88098	Vulnérabilité suivante résolue dans le noyau Linux : m
CSCwm88102	Vulnérabilité suivante résolue dans le noyau Linux : m
CSCwm88105	Problème découvert dans libexpat versions antérieures à 2.6.3. xmlparse.c ne fonctionne pas
CSCwm88133	Vulnérabilité suivante résolue dans le noyau Linux : P
CSCwm95191	Vulnérabilité suivante résolue dans le noyau Linux : s
CSCwm95208	Vulnérabilité suivante résolue dans le noyau Linux : r
CSCwm95242	Il existe une vulnérabilité de gravité MOYENNE touchant CPython. Regul
CSCwm95243	Il existe une vulnérabilité de gravité faible affectant CPython, en particulier
CSCwn03629	CVE-2022-48956 : linux-kernel : dans le noyau Linux, la vulnérabilité suivante...
CSCwn03654	CVE-2022-48978 : linux-kernel : dans le noyau Linux, la vulnérabilité suivante...

ID du bogue	En-tête :
CSCwn03663	CVE-2022-49002 : linux-kernel : dans le noyau Linux, la vulnérabilité suivante...
CSCwn31089	CVE-2022-48946 : linux-kernel : dans le noyau Linux, la vulnérabilité suivante...
CSCwn31092	CVE-2022-48949 : linux-kernel : dans le noyau Linux, la vulnérabilité suivante...
CSCwn31096	CVE-2022-48953 : linux-kernel : dans le noyau Linux, la vulnérabilité suivante...
CSCwn31100	CVE-2022-48969 : linux-kernel : dans le noyau Linux, la vulnérabilité suivante...
CSCwn31103	CVE-2022-48988 : linux-kernel : dans le noyau Linux, la vulnérabilité suivante...
CSCwn31116	CVE-2022-49010 : linux-kernel : dans le noyau Linux, la vulnérabilité suivante...
CSCwn31118	CVE-2022-49011 : linux-kernel : dans le noyau Linux, la vulnérabilité suivante...
CSCwn31121	CVE-2022-49015 : linux-kernel : correction possible d'utilisation après interruption de service dans netif_rx()
CSCwn31124	CVE-2022-49020 : linux-kernel : dans le noyau Linux, la vulnérabilité suivante...
CSCwn31125	CVE-2022-49021 : linux-kernel : dans le noyau Linux, la vulnérabilité suivante...
CSCwn31143	CVE-2024-38538 : linux-kernel : dans le noyau Linux, la vulnérabilité suivante...
CSCwn62940	CVE-2022-48695 : linux-kernel : dans le noyau Linux, la vulnérabilité suivante...
CSCwn62942	CVE-2024-26791 : linux-kernel : vulnérabilité de traitement du nom de volume btrfs
CSCwn62955	CVE-2024-26981 : linux-kernel : dans le noyau Linux, la vulnérabilité suivante...
CSCwn62982	CVE-2024-49962 : linux-kernel : dans le noyau Linux, la vulnérabilité suivante...
CSCwn62986	CVE-2024-49966 : linux-kernel : dans le noyau Linux, la vulnérabilité suivante...
CSCwn63018	CVE-2024-49995 : linux-kernel : dans le noyau Linux, la vulnérabilité suivante...
CSCwn63031	CVE-2024-50006 : linux-kernel : dans le noyau Linux, la vulnérabilité suivante...
CSCwn63032	CVE-2024-50007 : linux-kernel : dans le noyau Linux, la vulnérabilité suivante...
CSCwn63045	CVE-2024-50024 : linux-kernel : dans le noyau Linux, la vulnérabilité suivante...
CSCwn63049	CVE-2024-50035 : linux-kernel : dans le noyau Linux, la vulnérabilité suivante...
CSCwn63062	CVE-2024-50055 : linux-kernel : dans le noyau Linux, la vulnérabilité suivante...
CSCwn63065	CVE-2024-50058 : linux-kernel : dans le noyau Linux, la vulnérabilité suivante...
CSCwn63067	CVE-2024-50059 : linux-kernel : dans le noyau Linux, la vulnérabilité suivante...
CSCwn63084	CVE-2024-50095 : linux-kernel : dans le noyau Linux, la vulnérabilité suivante...
CSCwn63146	CVE-2024-50180 : linux-kernel : dans le noyau Linux, la vulnérabilité suivante...

ID du bogue	En-tête :
CSCwn63163	CVE-2024-50195 : linux-kernel : dans le noyau Linux, la vulnérabilité suivante...
CSCwn72848	La taille de la file d'attente db du fragment d'interface lina est incorrectement bloquée à 4294967295 - ASA/FTD

Dernière mise à jour du tableau : 22/05/2025

Tableau 25 : Bogues fonctionnels résolus dans la version 7.2.10

ID du bogue	En-tête :
CSCvj85665	Amélioration : Le nom d'hôte ou l'adresse IP de l'appareil doit être inclus dans les journaux système de FX-OS
CSCvu22491	FMC ne parvient pas à se connecter au SSM avec l'erreur « Failed to send the message to the server » (échec de l'envoi du message au serveur)
CSCvx66624	Le cache d'écriture est désactivé sur certains périphériques FMC M5
CSCvz03407	Le fichier IPTables.conf disparaît, ce qui entraîne un échec de la sauvegarde et de la restauration.
CSCvz85153	access-control-config n'affiche pas le nom de la politique NAP/IPS
CSCwb77894	Firepower 1000/2100 peut démarrer en mode ROMMON
CSCwc28374	Fonction de recherche d'une politique de contrôle d'accès de grande taille non en mesure de trouver les valeurs recherchées
CSCwc38383	Noyau Snort3 généré lors de l'activation de la journalisation CDB pour les débogages SSL
CSCwc57500	Suppression du paquet bootlogd de FXOS pour éviter les problèmes de journal de démarrage de l'appareil de sécurité adaptable
CSCwc70142	La suppression d'une interface EtherChannel en mode routé modifie les interfaces membres en mode de port de commutation
CSCwd06592	Le déploiement échoue en raison d'une configuration incorrecte avec une erreur de chargement impossible des règles
CSCwd08448	FMC devra fournir une alerte d'intégrité 60 jours avant l'expiration du certificat cacert.pem
CSCwd49767	La fenêtre contextuelle du système est vide pour les utilisateurs de l'administrateur de réseau et de l'approbateur de sécurité
CSCwe42986	Les événements classiques et unifiés doivent gérer les cas où SMC est inaccessible
CSCwe60267	Défaillance de FXOS F0853 et F0855 observées malgré le renouvellement du rapport de certificats de trousse de clés

ID du bogue	En-tête :
CSCwe63686	Échec de la préparation de la mise à niveau dans WM FDM @009_check_snort_preproc.sh, mais la mise à niveau vers la version 7.3.1-19 a réussi
CSCwe79990	Flux de renseignements Cisco – Échec du téléchargement en raison d'un délai d'expiration
CSCwe88492	La bannière de connexion ne s'affiche pas lorsqu'elle est configurée
CSCwe92324	FPR31xx – L'interrogation SNMP signale un état incorrect du tiroir de ventilation en panne alors qu'il est actuellement opérationnel
CSCwe93925	Le déploiement échoue sur FTD lors de la réutilisation ou de la réaffectation d'un ID de VLAN existant à une interface différente
CSCwe98559	Snort3 – compteurs nécessaires manquants pour les statistiques d'ARN
CSCwf04460	Le répertoire FXOS disparaît après l'annulation de l'exécution de la commande afficher les détails FPRM avec Ctr+c.
CSCwf04983	Échec d'ajout de l'unité 3100 à la grappe avec l'erreur « configured object (sys/switch-A/slot-2) not found ».
CSCwf17314	Les journaux de déploiement de FMC tournent plus rapidement en raison de /internal_rest_api/accesscontrol/rapplicationsavailable
CSCwf25454	Entrées AnyConnect périmées provoquant des problèmes de routage
CSCwf42097	Le micrologiciel PSEQ (Power-Sequencer) ne peut pas être mis à niveau avec la mise à niveau groupée de FXOS
CSCwf66818	Le tableau de bord de supervision VPN FMC affiche incorrectement le FTD en veille comme propriétaire de session VPN dans la paire à haute disponibilité
CSCwf78497	Migration de flexconfig EIGRP 7.2.0, aucune interface de ligne de commande ne doit être migrée s'il ne s'agit pas de la configuration par défaut
CSCwf80183	Noyau Snort3 dans la navigation vu pendant le flux du trafic
CSCwf84200	Noyau Snort lors de l'exécution des statistiques de flux IP
CSCwf92371	Unité secondaire à haute disponibilité désactivée après le redémarrage – Le gestionnaire de processus n'a pas réussi à sécuriser le LSP
CSCwh01312	ENH : L'authentification extérieure FMC ne fonctionne pas pour SSH lorsqu'elle est configurée avec IPv6.
CSCwh11411	Snort : Trafic de liste noire pendant le déploiement
CSCwh13182	FTD : Échec de la mise à niveau de la version 7.2.4 à la version 7.4.1 et échec de la restauration pour sortir le périphérique du mode maintenance
CSCwh15109	L'installation de la SRU est bloquée dans le script 602_log_package.pl, ce qui entraîne l'échec du déploiement

ID du bogue	En-tête :
CSCwh17965	[Afficher]FXOS : L'interface membre de PC s'affiche comme en panne et non associée/non attribuée après le rechargement
CSCwh23124	Le nœud secondaire/de secours affiche un basculement entre l'état prêt et l'échec lorsque l'interface de gestion est fermée
CSCwh25406	Snort3 : Noyau lors de l'exécution du trafic continu IMS 7.4.1-73
CSCwh29167	FMC FlexConfig réorganise les objets après un seul déploiement réussi
CSCwh36167	DAP : FMC ajoute des caractères  dans un script LUA
CSCwh36328	Les paramètres de configuration de l'outil de test sont partagés par HTTP et HTTP/2, ce qui entraîne une situation de concurrence - test de régression uniquement
CSCwh37655	Snort2 : Ignorer l'écriture du fichier d'origine des programmes malveillants en raison de l'arrêt du processus
CSCwh41126	Le rapport FMC ACP n'affiche pas toutes les règles de contrôle d'accès
CSCwh41606	Une journalisation étendue pour un déploiement problématique a entraîné le remplacement des journaux importants
CSCwh46732	Échec du trafic du bureau à distance (RDP) lorsque TSID est activé
CSCwh49085	Évite les opérations de base de données inutiles lors du traitement des empreintes dérivées
CSCwh58190	Échec de déploiement de FMC dans csm_snapshot_error
CSCwh61832	FDM : Autoriser l'activation ou la désactivation de l'interrogation de mempool GSP par l'intermédiaire de Flexconfig
CSCwh63663	Impossible d'utiliser le domaine .k12 sur la configuration du domaine AD principal
CSCwh66315	En ce qui concerne la présence de modules d'intégrité (état PEP, moniteur de processus de pulsation) dans FMC
CSCwh70639	FTD : L'installation de la mise à jour a échoué. nom de domaine : RPC refusé : autorisation refusée (rôle=manager) pour le nom de domaine homologue
CSCwh75829	Erreur de dégradation du disque principal du FMC
CSCwh78064	FTD : Le script de mise à niveau essentiel ne doit pas être contourné par la nouvelle tentative de mise à niveau
CSCwh83854	Impossible de configurer la règle de corrélation, car il n'y a aucune valeur pour le GID qui dépasse 2 000
CSCwh85824	Erreur d'analyse JSON eStreamer et fuite de mémoire
CSCwh87058	FTD : Résultats de la génération de certificats internes entraînant une non-concordance entre le certificat et la clé privée

ID du bogue	En-tête :
CSCwh92541	Recherche de la source aléatoire de Snort3 sur FTD
CSCwh95003	Le processus d'initialisation atteint 100 % d'utilisation du processeur après un échec de sauvegarde
CSCwh96088	Utilisation élevée du disque non géré sur FMC/ volume en raison de fichiers MonetDB volumineux – FMC 7.2.4
CSCwi02039	Le script FMC Clean_revert_backup échoue en silence sans créer de journaux
CSCwi05709	Redémarrage de FTD en raison d'un événement de système de fichiers
CSCwi08392	La configuration /32 crée l'adresse PPPoE : « Valeur non valide de l'adresse IPV4 ou chevauchement du sous-réseau ou du réseau »
CSCwi16571	Commande capture-trafic Clish avec snort3 ne produit pas de capture résultante appropriée
CSCwi18663	FMC-4600 : La politique de préfiltre ne s'affiche pas
CSCwi19485	Le mode fail-open de Snort-down est désactivé dans les paires en ligne, bien qu'il soit activé et déployé depuis le FMC
CSCwi21909	FMC : Affichage de « missing en-US:BGP » via l'Aperçu du déploiement lorsque les modifications de BGP ont été annulées
CSCwi27093	Erreur FMC pour un réseau IPv4 non valide ou un littéral d'hôte du groupe lors de l'ajout d'un réseau dans l'ACP
CSCwi28645	L'utilisateur affecté à un rôle personnalisé en lecture seule n'est pas en mesure d'afficher le contenu de la politique de prévention des intrusions pour snort2
CSCwi38708	Échec du déploiement de FDM
CSCwi40674	Le profil Umbrella et d'autres ont été effacés incorrectement lors de la modification de la politique de groupe dans l'interface utilisateur
CSCwi41666	Amélioration du démarrage de MonetDB pour le nettoyage des fichiers volumineux
CSCwi44007	Échec de la validation FMC pour une grande plage d'objets et réussite pour le réseau d'objets dans NAT64
CSCwi45408	Monetdb ayant 14 Go de données BAT inconnues ce qui provoque une « utilisation élevée du disque non géré sur /Volume »
CSCwi46676	API :/operational/commands ne fonctionnent pas comme indiqué par swagger
CSCwi49128	Mettre à jour les journaux – Sérialisation des objets SSP pendant la haute disponibilité
CSCwi51611	FTD 7.4.1 Snort affiche 100 % d'utilisation, même à un faible débit de trafic
CSCwi52623	Vérification incorrecte des attributs de certificat selon les critères pour les terminaux DAP

ID du bogue	En-tête :
CSCwi54926	Dans une paire FMC à haute disponibilité, le « moniteur d'intégrité » peut afficher des rôles incorrects lorsque l'unité secondaire est active.
CSCwi55009	Erreur lancée si l'utilisateur de Security Analytics tente d'accéder à la page de saisie de paquets
CSCwi56733	Erreur interne lors de la tentative de configuration de PBR dans FMC
CSCwi58187	Limite de seuil d'avertissements NAT incorrect de 131 838 adresses IP
CSCwi59453	Démarrage après l'échec de la mise à niveau – Reprendre la haute disponibilité avec un motif où le déploiement existe déjà
CSCwi67510	FMC : Traceur de paquet affichant une erreur « Interface not supported » pour les interfaces VLAN
CSCwi67638	La règle DAP configurée pour FMC avec les attributs SAML IDP Azure ne correspond pas
CSCwi69260	La mise à niveau de FMC vers la version 7.2.x supprime l'authentification EIGRP fournie par FlexConfig des interfaces sur les FTD
CSCwi78941	Le déploiement FDM échoue avec l'erreur « Certaines interfaces ont été ajoutées ou supprimées de l'appareil »
CSCwi82866	Les déclencheurs de moniteur MonetDB pour le redémarrage de MonetDB en fonction de la taille de WAL ne sont pas efficaces
CSCwi92702	La fonction Exécuter tout sur la page de surveillance de l'intégrité du FMC est grisée après la mise à niveau
CSCwi93186	Le provisionnement sans intervention échoue à l'étape initiale de provisionnement
CSCwi94356	Rechargement avec recherche de la source de Lina dans le nom de fil 'cli_xml_request_process'.
CSCwi97667	L'état de synchronisation de FMC à haute disponibilité affiche un échec lors de l'installation de VDB/SRU sur les appareils FMC actif et en veille
CSCwi98147	Tomcat redémarre au milieu du flux LTP en raison d'une mise à jour de certificat
CSCwj02259	Les échecs de sauvegarde doivent être affichés avec l'état correct sur l'interface GUI
CSCwj03112	pmttool restart of monetdb (redémarrage pmttool de monetdb) ne parvient pas à afficher monetdb, trop de fichiers dans le répertoire de volume monetdb
CSCwj03285	FMC : L'alerte du moniteur d'intégrité n'est pas correctement émise concernant l'utilisation du disque
CSCwj03876	La suppression de la règle IPS Snort 3 ne génère pas de journal d'audit
CSCwj05464	Le certificat du serveur FMC n'affiche que les 20 premiers objets

ID du bogue	En-tête :
CSCwj08203	FMC : Fireamp générant trop de journaux
CSCwj10923	FTD – Problèmes de connectivité instable de sftunnel lorsque le contrôle et l'événement sont configurés dans le même sous-réseau
CSCwj14242	Les applications sont incorrectement identifiées comme TOR et bloquées par Snort3
CSCwj14589	Alerte d'échec d'inscription SSE de configuration de nuage FMC-SSE en raison d'un fichier connecteur.toml vide sur le FTD
CSCwj14798	Le processus TSS_Daemon se termine chaque minute
CSCwj16119	FP2110 : Échec de la sortie de l'API de la plateforme en mode « On-Box » (FDM)
CSCwj17852	FMC – Le menu de politique de base de la sélection des paramètres hérités disparaît lors du défilement à l'aide de l'interface utilisateur claire ou crépuscule
CSCwj17969	rna_ip_os_map peut devenir très volumineux et entraîner l'arrêt du traitement des événements par SFDataCorrelator
CSCwj23777	Colonne(s) manquante(s) dans le tableau eventdb
CSCwj24517	Échec du déploiement du LSP dans plusieurs instances FP 41xx/93xx
CSCwj26204	les périphériques de sauvegarde FMC restaurés s'affichent comme « normaux » et « intègres », bien que sans connexion avec le FMC
CSCwj26595	FMC permet le chargement d'un certificat binaire dans l'objet d'authentification extérieure
CSCwj30582	La page des mises à jour de géolocalisation devrait générer une erreur dans le cas où le site d'assistance est inaccessible
CSCwj31904	Après la mise à niveau, le déploiement de FDM échoue « Délai d'attente pour les moteurs de détection de SNORT pour traiter le trafic »
CSCwj33503	Les PCAP d'événements Snort3 contiennent uniquement des données d'en-tête lors du déchiffrement HTTP/2
CSCwj34374	Échec de l'enregistrement de SecureX / plateforme Cisco Security Cloud si FMC se trouve derrière un serveur mandataire
CSCwj39184	FDM /ngfw/var/sf/fwcfg/zones.conf est vide pour la version 7.3.1
CSCwj39212	Croissance de la mémoire SFDataCorrelator lors du traitement d'un nombre élevé d'identités d'utilisateurs expirées
CSCwj44464	La règle ACP peut ne pas être appliquée après le déploiement ou l'échec du déploiement en raison d'une incompatibilité de fuseau horaire FXOS- FTD
CSCwj45075	Les processus critiques s'affichent deux fois après la mise à niveau à la version 7.0.6.x

ID du bogue	En-tête :
CSCwj45351	Impossible d'ajouter des mappages d'attributs LDAP supplémentaires sur le FMC mis à niveau
CSCwj45439	Erreur d'importation de certificat interne : échec de validation EO basé sur les certificats : type de clé non pris en charge
CSCwj48308	Alertes d'intégrité périmées vues sur l'UMS après la migration du modèle
CSCwj50557	Snort crée trop de fichiers journaux unifiés par Snort lors des déploiements fréquents de politiques
CSCwj51115	Échec de la copie de sauvegarde du serveur distant de FMC vers le serveur distant de Solar Winds après la mise à niveau vers les versions 7.x
CSCwj54042	Modifications de l'ordre de séquence des politiques de chiffrement IKEv2 lors des modifications de configuration de l'interface et de la sous-interface
CSCwj56668	Erreur d'alerte de téléchargement en bloc ISE sur FMC
CSCwj57435	Nettoyage des fichiers logrotate périmés
CSCwj58442	L'état de HA de FTD dans le FMC sur site est corrompu, signalant le secondaire comme principal
CSCwj61086	Utilisation élevée de l'UC dans le processus svc_sam_dme lors du déploiement après l'interruption de la grappe ou la suppression de l'ensemble en ligne
CSCwj62959	Échec du déploiement et restauration lors du changement de parent de la sous-interface avec adresse MAC de basculement
CSCwj63921	Recherche de la source Snort3 et rechargement en raison d'une corruption de mémoire dans le module de fichiers
CSCwj65811	FMC est inondé de messages « Impossible de trouver l'ID de règle SSL pour la politique » si la découverte d'identité du serveur TLS est activée
CSCwj69358	Veuillez fournir des messages sur FMC 7.2 et 7.3 indiquant que la nouvelle interface utilisateur de ACP n'est pas destinée à une utilisation évolutive ou permanente
CSCwj72013	La communication PAT par le biais du bassin PAT échoue pendant environ 40 secondes lorsqu'un périphérique rejoint une grappe
CSCwj72721	Échec du déploiement et restauration lorsque les communautés de BGP sont ajoutées ou supprimées dans la clause de correspondance de carte de routage
CSCwj73171	Snort3 : Les paquets de plus petite taille dépassant la limite maximale de segments entraînent un blocage de Snort
CSCwj79736	Fuite de mémoire dans eStreamer lorsque le FMC reçoit des événements de FTD gérés par CDO
CSCwj85103	Impossible de télécharger le groupe/l'utilisateur en raison d'une erreur de syntaxe SQL dans les index de recreation

ID du bogue	En-tête :
CSCwj89228	Utilisation du disque FTD/mnt 100 % en raison des fichiers de mémoire mappée Snort
CSCwj91420	Snort3 se bloque lors de la collecte du profilage IP de flux
CSCwj98451	FMC a été désinscrit de la licence Smart après la mise à niveau
CSCwj98872	eth0 peut ne pas être correctement initialisé après le redémarrage
CSCwk04216	Échec de téléchargement de domaine avec le processus ADI n'est pas disponible actuellement
CSCwk04893	FTD ne compacte pas les fichiers utilisés pour communiquer les mises à jour des mappages SGT/IP
CSCwk04908	FTD Impossible d'enregistrer auprès du FMC en raison d'un serveur DNS vide configuré.
CSCwk06216	Perte du mappage d'interface avec les zones de sécurité après le déploiement
CSCwk07250	La mise à niveau de FMC échoue lors de l'exécution du script 120_check_legacy_private_cloud_for_ampkit.pl
CSCwk07563	Forcer le déploiement sans générer de nouveau le cache d'exportation dans le périphérique
CSCwk08064	Retards de traitement de session ADI de nouveau après la mise à niveau à la version 7.2.x
CSCwk09559	FMC - Le rôle d'utilisateur personnalisé VPN permet à l'utilisateur d'apporter des modifications au VPN de site à site lorsque la case Modifier n'est pas cochée.
CSCwk11254	« Rule Unavailable » (Règle non disponible) pour certaines règles de prévention des intrusions locales peut être affichée dans la vue des paquets des incidents d'intrusion
CSCwk11989	Acceptation de l'objet/groupe-objet en double dans le groupe-objets à partir de plusieurs sessions SSH
CSCwk12337	Les chiffrements RC4 ne peuvent pas être désactivés sur FMC/FTD pour l'authentification de portail captif avec Kerberos
CSCwk21533	La page des utilisateurs FMC dans le sous-domaine ne se charge pas
CSCwk22814	FMC – Ajout d'un message d'avertissement lors de la configuration du MTU CCL
CSCwk24380	Aucun périphérique répertorié dans la liste déroulante « Sélectionner un périphérique » du traceur de paquets
CSCwk24440	Les sauvegardes peuvent échouer sur le stockage distant lorsque le contenu du filebackup.tar est si volumineux
CSCwk25506	Plusieurs fichiers binaires snort sont présents (correctif ou HI) à l'adresse /var/sf/bin/, ce qui fait échouer la commande tar

ID du bogue	En-tête :
CSCwk28058	Épuisement de la mémoire du Cisco FTD ce qui entraîne une recherche de la source et un rechargement
CSCwk30049	ASA/FTD Peut effectuer la recherche de la source et le recharger en citant le nom de fil « lina » comme fil défectueux.
CSCwk30965	AppIdSessionData entraîne le plantage de snort3 dans la version 7.2.6
CSCwk33387	Le protocole SNMP pour le trafic sortant mgmt0/diagnostic est manquant
CSCwk33516	MonetDB en panne en raison d'un tableau corrompu (colonnes manquantes dans le tableau)
CSCwk34905	Alertes d'intégrité de l'état de la connexion ISE sur FMC avec services ISE en panne
CSCwk36860	Paquets de tunnel IPv6 vers la source de tunnel DVTI sur la boucle de retour VRF abandonnés (acl-abandon)
CSCwk38440	Si conn_meta est nul, ne pas envoyer de paquets à snort
CSCwk38851	FMC ne doit pas effectuer de sauvegarde de politique lors de l'installation de correctifs ou de correctifs rapides.
CSCwk40403	Le trafic WebEx n'est pas contourné dans snort3 (règles d'autorisation)
CSCwk41396	La migration de l'appareil de sécurité adaptable vers le FTD par le biais de FMT entraîne une configuration incorrecte des groupes d'interfaces dans la configuration du système dorsal FMC
CSCwk41806	Nécessité de protéger LINA pour qu'elle ne soit pas tuée par OOM
CSCwk42266	La règle AC basée sur la zone a un mappage d'interface manquant
CSCwk42676	ASA/FTD virtuel peut rechercher la source et recharger dans le nom de fil « PTHREAD »
CSCwk46737	ASA sur la haute disponibilité : alloc_ch() alloc du message d'échec du fragment mem sur un contexte dans le périphérique de secours
CSCwk48628	FTD/FxOS – La mise à niveau ou l'effacement entraîne dans l'instance d'application « État opérationnel : démarrage »
CSCwk54033	FMC ne peut pas se connecter à l'AMP privé lorsque le serveur mandataire est activé dans l'interface de gestion
CSCwk63586	Instance d'application bloquée dans STOP_FAILED avec un message d'erreur
CSCwk67346	Les politiques DAP ne fonctionnent pas avec l'attribut TRUE/FALSE (vrai/faux)
CSCwk71227	FTD fonctionnant sur FPR 2k avec LDAP ignore la barre oblique lors de la mise à jour de ldap.conf

ID du bogue	En-tête :
CSCwk78075	FTD ne marque pas les déploiements en cours bloqués comme échoués, ce qui entraîne des échecs de déploiement ultérieurs
CSCwk78242	Attributs d'utilisateur vides dans LDAP entraîne un téléchargement partiel de l'utilisateur/groupe
CSCwk78393	Amélioration de la journalisation pour les erreurs LDAPS SSL
CSCwk86563	Le port source et le port de destination sont permutés lors de l'évaluation du SID
CSCwk88913	Conserver une sauvegarde FMC localement jusqu'à ce que nous copions le fichier sur le serveur distant avec succès
CSCwk89127	La table Backup_info n'est pas nettoyée, ce qui entraîne un ralentissement des requêtes DB
CSCwk94697	FMC permet de téléverser un certificat binaire dans l'importation du certificat d'identité
CSCwk97058	FMC – La validation du prédéploiement devrait signaler une erreur et bloquer le déploiement si le certificat VPN est en état d'échec
CSCwm03227	Échec de la mise à niveau de FTD en raison de plusieurs dossiers de base de données dans le chemin /ngfw/var/cisco/deploy/tmp_bundle/db/
CSCwm05196	Lors de l'utilisation d'un objet basé sur le temps dans ACP, l'événement ne s'affiche pas dans FMC
CSCwm05221	Échec de la détection du fichier Snort3 avec un trafic dissymétrique en mode passif IDS
CSCwm06393	Les modifications apportées à l'appartenance au canal de port ou à l'état des membres peuvent entraîner des basculements périodiques de l'adjacence OSPF/EIGRP
CSCwm27588	Le correctif pour supprimer les caractères d'espace dans les noms d'objets authentifiés lors de la mise à niveau de FMC peut entraîner l'échec de cette dernière
CSCwm28007	Le navigateur redirige vers une page vide lorsque l'utilisateur clique sur le signet WebVPN
CSCwm29768	La connexion a été journalisée pour les règles sans journalisation activée
CSCwm29929	L'éditeur de politique QoS sur l'interface GUI de FMC n'a pas de pagination fonctionnelle lorsque la politique QoS comporte plus de 50 règles
CSCwm30731	La table de routage OSPF de l'ASA n'est pas correctement synchronisée avec les voisins
CSCwm33529	Le traitement FXOS MTU pour les ports du panneau avant et de liaison ascendante des appareils Firepower nécessite une amélioration
CSCwm33613	La politique de groupe par défaut est appliquée lors de la réception de plusieurs politiques de groupe dans les attributs d'assertion SAML

ID du bogue	En-tête :
CSCwm33619	Le processus FTD Vault se termine toutes les 1 minutes : « Process vaultApp (23597) a été abandonné normalement : 256 »
CSCwm35051	Le champ du nom d'hôte/adresse IP n'accepte pas les domaines se terminant par un chiffre
CSCwm35251	FMC4700 affiche des alertes de vitesse de ventilateur prématurées
CSCwm35730	LINA peut effectuer une recherche de la source dans le nom du fil : chemin de données avec configuration NAT
CSCwm35751	FPR3100 : L'interface peut passer à la vitesse de demi-duplex, codée en dur à 100 Mbit/s
CSCwm36631	L'unité secondaire FTD est bloquée dans l'état de synchronisation en bloc.
CSCwm37043	Notification du gestionnaire de plantage pour la défaillance de SNORT3 non envoyée dans la configuration MI
CSCwm37455	L'appareil de sécurité adaptable/FTD autorisera le regroupement d'adresses IP locales avec un masque réseau non valide
CSCwm37690	Les règles NAT sont supprimées avant l'enregistrement de la politique sur FMC
CSCwm38635	Le trafic TACACS+ est abandonné par l'identité du serveur TLS dans le module XTLS
CSCwm40278	S2S VPN supprimée de manière inattendue après le déploiement
CSCwm41381	Le téléchargement de fichier échoue par intermittence avec les programmes malveillants et la politique de fichiers configurés
CSCwm41847	Convivialité pour capturer le bloc d'écriture/lecture PDTS pour aider la cause première CSCwm36314
CSCwm42000	FTD/ASA peut effectuer une recherche de source et recharger dans le fil DataPATH
CSCwm44412	FTD inline-set ignore l'indicateur inverse pour l'injection/la réécriture
CSCwm47775	Échec du déploiement de FMC lors de la modification de la politique de NAT avec allocation de blocage et tourniquet activés
CSCwm49154	Défaillance FXOS F1738 vue dans le déploiement avec l'erreur : CSP_OP_ERROR Erreur de vérification de la signature CSP
CSCwm49721	Recherche de la source et rechargement de l'appareil de sécurité adaptable en raison d'une corruption de la mémoire
CSCwm49782	enhance sma 2nd cruz heartbeat logging (amélioration de la journalisation de sma 2nd cruz heartbeat)
CSCwm50591	ASA/FTD : Les paquets IPsec entrants sont abandonnés lorsque le déchargement IPsec est activé avec le VTI et la sous-interface

ID du bogue	En-tête :
CSCwm51747	Échec d'accès SSH avec authentification par clé publique après la mise à niveau de FXOS
CSCwm51874	FXOS : les messages sont soumis à une rotation toutes les 40 minutes en raison de l'envoi de pourriels par le démon de notification
CSCwm51923	Transcription de déploiement affichant « Enable management access: false »
CSCwm52264	Impossible d'effectuer le retrait ou l'effacement de la défaillance « La clé de chiffrement du mot de passe n'a pas été définie ».
CSCwm52931	ASA/FTD peut effectuer une recherche de la source et un rechargement dans le nom de fil « fover_parse »
CSCwm56864	show run access-list command returns warning (afficher l'exécution de la commande access-list renvoie un avertissement)
CSCwm57511	Problèmes d'exécution d'Omniquery dans extdb
CSCwm58260	Le plantage Snort3 sur le certificat TLS a le même émetteur et le même nom commun, mais l'algo de signature et la clé publique sont différents
CSCwm58772	Les instances Snort2 redémarrent de manière inattendue avec OOM lors du déploiement de la politique
CSCwm60536	Le trafic SQLNet est abandonné par intermittence dans l'unité de données de mise en grappe.
CSCwm61282	ASA/FTD : Tunnel VPN d'accès à distance causant une fuite de mémoire entraînant une recherche de la source et un rechargement
CSCwm63868	FTD – Routes manquantes sur les routes annoncées par BGP après l'événement de basculement à haute disponibilité de FTD
CSCwm65693	Les règles Snort 3 affichent une différence dans l'interface graphique de FMC.
CSCwm65773	L'actualisation de l'inventaire affiche un message incorrect « L'appareil n'est pas accessible » alors que sftunnel est activé
CSCwm66731	Dans l'action de modification de politique RAVPN bloquée, lors de l'édition des mappages d'attributs LDAP
CSCwm67414	Impossible de modifier/supprimer le module client dans la politique de groupe RAVPN
CSCwm68211	Recherche de la source ASA et rechargement sur le fil snmp_inspect
CSCwm69907	FMC n'envoie pas ou ne synchronise pas le fichier de configuration RADIUS aux FTD
CSCwm70835	Recherche de la source et rechargement de l'ASA en raison d'un débordement de la pile lors de l'utilisation du fichier APCF

ID du bogue	En-tête :
CSCwm71265	Recherche de la source ASA et rechargement sur le fil DataPATH lors du traitement du message du marqueur de fin gtpv1 pour PDP
CSCwm72757	Snort3 bloque le trafic ESMTP par intermittence et déclenche les signatures SAI 124:3:2 et 124:1:2
CSCwm74289	Les dérouterments NAT doivent être limités en débit
CSCwm77673	Déploiement de la politique bloqué à 5/8 % - Collecte de politiques et d'objets
CSCwm78351	Utilisation élevée potentielle de l'UC dans la configuration de la grappe multi-contexte avec exécution inconditionnelle du code de capture
CSCwm79920	L'utilisateur d'authentification externe (RADIUS) n'a pas pu se connecter à FTD en raison de cas non concordants lors de la connexion initiale
CSCwm82683	Le nettoyage de l'enregistrement ne doit pas s'exécuter si le répertoire des homologues ne peut pas être ouvert
CSCwm85228	ASA/FTD peut rechercher la source et se recharger dans le nom de fil « IKEv2 Daemon » lors de la jonction du basculement
CSCwm86416	Amélioration : API FMC : options de mise à niveau de défense contre les menaces ignorent la génération automatique des fichiers de dépannage
CSCwm89523	« no capture /all » n'a pas réussi à désactiver complètement la capture dans le serveur principal, ce qui entraîne un processeur de données élevé
CSCwm90905	L'inspection GTP abandonne le paquet avec l'erreur ERROR-DROP:MsgType:32
CSCwm92397	Noyau LINA observé pointant vers le fil « IP RIB Update »
CSCwm93119	FMCv est incompatible avec certaines versions logicielles d'hyperviseur KVM
CSCwm95116	Plantage de l'ADI sur FTD en raison du fait que les deux ADI de FMC ne sont pas désactivés
CSCwm95328	Copier/ coller pour une règle sur n'importe quelle page d'interface utilisateur autre que la page 1 entraîne le chargement de l'interface utilisateur de politique à la page 1.
CSCwm96280	Périphérique FTD bloqué en mode rommon après avoir enfoncé le bouton de réinitialisation
CSCwm96652	Grappe attribuant une mauvaise NAT à l'unité, le trafic n'est pas renvoyé correctement vers l'unité
CSCwm97054	Recherche de la source ASA/FTD et rechargement avec un taux élevé de connexions SIP
CSCwm98278	La connexion TCP n'est pas signalée comme partiellement fermée après avoir reçu l'accusé de réception pour le FIN.
CSCwn00475	Fuite des blocs de mémoire 80 et 9344 en raison de la priorité de la file d'attente

ID du bogue	En-tête :
CSCwn01281	Inspection GTP n'autorise pas les paquets de données GTP si la réponse de création de session a le type de cause 18
CSCwn03446	Lorsque la capture est activée sur l'interface de grappe, elle inclut toujours l'adresse IP CCL ainsi que la règle configurée
CSCwn03796	Inscription de style d'unité après l'enregistrement sur le portail AMPkit
CSCwn03835	ASA/FTD peut effectuer un rechargement avec recherche de la source dans le nom de fil « SSH Ctxt Thread »
CSCwn05183	Les interfaces du nœud actif de la haute disponibilité FTD sont tombées en panne après l'échec du déploiement de la politique
CSCwn10538	ADI sur FTD ne s'arrête pas après un plantage
CSCwn13187	Échec de la mise à niveau de l'appareil de sécurité adaptable de la version 9.20.2.21 à la version cible 9.20.3.4
CSCwn14130	La grappe FTD peut effectuer un rechargement avec recherche de la source après l'activation de la PAT étendue
CSCwn14447	ASA/FTD peut effectuer un rechargement avec recherche de la source dans le nom de fil « ldap_client_thread »
CSCwn15104	Rechargement FTD avec recherche de la source sur la fonction swapcontext
CSCwn15589	Besoin d'un paquet ou d'un correctif unifié pour pseq et du correctif rommon associé pour l'échec de la mise à niveau de pseq
CSCwn17121	ASA/FTD peut effectuer un rechargement avec recherche de source dans le nom de fil « cli_xml_request_process ».
CSCwn19498	Impossible d'ajouter des nœuds de données à la configuration de la grappe existante pendant la phase de synchronisation des applications de grappe
CSCwn19706	Les administrateurs sont invités à modifier le mot de passe local lors de l'authentification auprès du serveur externe
CSCwn19739	La haute disponibilité mettrait en service les interfaces de données lors du passage de l'état de secours froid à l'état de défaillance
CSCwn20024	ASA peut rechercher la source et recharger dans le nom de fil « ssh »
CSCwn22036	FTD: État de Management0/0 en panne, le protocole de ligne est activé après la mise à niveau
CSCwn22456	GTPv2 IE-type 157 (signalisation de la priorité de signalisation) est abandonné avec raison comme type IE inconnu
CSCwn23992	Les messages d'envoi, y compris UMS, sont interrompus lorsque le FMC est atteint sur le port 443

ID du bogue	En-tête :
CSCwn24577	Le processus de démarrage de l'appareil de sécurité adaptable peut se bloquer lors de l'inclusion de la configuration « no pim » ou « no igmp »
CSCwn26165	FTD/ASA peut effectuer la recherche de la source et le rechargement - Pendant le déploiement/modifications Radius - En raison de paquets Radius
CSCwn27819	Les paquets de trames étendues sont fragmentés
CSCwn31653	FTD peut effectuer une recherche de source et recharger dans le nom de fil « FPRLI_FPR4K-SM-32 »
CSCwn34259	Interfaces surveillées peuvent passer à l'état d'attente après la mise à niveau vers la version 9.20.3.7
CSCwn34659	Le pare-feu ne lance pas la demande TCP, même après avoir reçu le bit TC défini dans la réponse DNS
CSCwn34707	Plusieurs processus Unicorn Admin Handler consomment toute l'unité centrale du plan de commande.
CSCwn35470	Convivialité : prise en charge de la trace de débogage et de capture de paquets FQDN
CSCwn39780	Résilience du déploiement FTD : ignorez les commandes non critiques ou inexistantes pour éviter les échecs de déploiement.
CSCwn39826	La haute disponibilité devrait empêcher de répondre aux demandes de basculement pendant que la copie/la synchronisation/la restauration est en cours.
CSCwn40572	MI : les informations sur le VLAN ne sont pas appliquées au niveau de FXOS lorsque la MAC virtuelle est configurée
CSCwn42949	Mise en œuvre du flux de transfert sur des unités non-propriétaires qui gèrent les connexions de flux secondaire distribuées
CSCwn44335	FXOS – La commande de téléchargement génère un « / » supplémentaire pour les demandes HTTP et HTTPS GET
CSCwn45510	Échec de la renégociation réussie de la SA enfant du tunnel VPN S2S
CSCwn46855	LINA peut observer une recherche de source aléatoire avec NetFlow configuré
CSCwn47308	Alertes d'intégrité critiques « user configuration(FSM.sam.dme.AaaUserEpUpdateUserEp) » sur FPR 1100/2100/3100
CSCwn54561	Modifier l'allocation de mémoire pour le sous-groupe de déploiement des politiques
CSCwn54966	Snort3 : Trafic TCP intermédiaire sur ACK normalisé par Snort et bloqué par le préprocesseur de flux
CSCwn63839	Recherche de la source dans le nom de fil Lina lors de la configuration d'arp allow-nonconnected avec les BVI

ID du bogue	En-tête :
CSCwn65415	ASA : connexion flottante ne ferme pas les connexions UDP si la connexion a été créée sans entrée ARP pour le prochain saut
CSCwn73318	Le graphique du moniteur d'intégrité FMC (HM) affiche un nombre incorrect de cœurs de CPU Snort et System
CSCwn73351	L'option de fuseau horaire Asie/Bangkok n'est pas répertoriée dans l'appareil de sécurité adaptable fonctionnant sur firepower1k
CSCwn75667	La bannière motd ne s'affiche pas lorsqu'elle est configurée
CSCwn75744	Après la mise à niveau de FMC, le déploiement échoue en raison d'objets SI élevés
CSCwn76079	SSH fonctionne dans le contexte de l'administrateur, mais ne fonctionne dans aucun contexte d'utilisateur après avoir modifié l'échange de clé SSH
CSCwn78846	Recherche de la source Snort3 et rechargement pendant le rechargement de l'identité de l'utilisateur
CSCwn79553	Les références LDAP/AD inaccessibles peuvent entraîner des retards ou des délais d'expiration dans l'authentification extérieure sur FTD
CSCwn80400	Vitesses de téléchargement lentes avec AnyConnect sur TLS sur les réseaux à latence élevée
CSCwn80765	ISA3000 avec ASA refuse l'accès SSH si CiscoSSH est activé
CSCwn84557	Recherche de la source sur Lina et rechargement en raison de « spin_lock_fair_mode_queue »
CSCwn86002	core corruption still seen with switching to quick core feature (corruption du noyau toujours observée avec le passage à la fonctionnalité de noyau rapide)
CSCwn90900	Utilisation élevée de la mémoire ASA/FTD en raison de l'interrogation des OID SNMP liés au VPN d'accès à distance
CSCwn92894	Parfois, la sortie « show chunkstat top-usage » n'affiche pas toutes les entrées
CSCwn93319	ASA/FTD peut rechercher la source et recharger dans le nom de fil « DATAPATH »
CSCwo01557	Recherche de la source et rechargement ASA sur le fil DATAPATH en raison d'une corruption de la mémoire
CSCwo06959	Le blocage des programmes malveillants ne se produit pas en raison d'un délai d'attente de la recherche dans le nuage des programmes malveillants
CSCwo08042	ASAv rechargé de manière inattendue avec recherche de la source sur le fil du serveur mandataire Unicorn
CSCwo09060	Point de confiance SSL avec des clés RSA de 4 096 bits non autorisé par l'appareil de sécurité adaptable si renouvelé via l'interface de ligne de commande
CSCwo09618	Échec de l'activation des débogages avec EEM

ID du bogue	En-tête :
CSCwo13863	Snort3 a planté parce que le bit ne pas fragmenter était défini et il n'a pas traité les fragments IPv4 comme des fragments
CSCwo16016	Les utilisateurs du serveur RADIUS existant peuvent se connecter au domaine FMC en veille lorsque MA est activé
CSCwo35585	Alerte d'intégrité associée à AMP lors de la mise à niveau et faute de frappe dans le message d'alerte
CSCwo41250	Recherche de la source et rechargement dans le fil nommé : DATAPATH-1-23988 en cas de condition de mémoire faible
CSCwo42139	Recherche de la source Snort3 et échec du déploiement avec la mise à niveau VDB
CSCwo77662	Certains caractères spéciaux ou espaces dans les mots de passe d'utilisateur RADIUS entraînent un échec de connexion dans FMC

Bogues résolus dans la version 7.2.9

Dernière mise à jour du tableau : 22-10-2024

Tableau 26 : Bogues résolus dans la version 7.2.9

ID du bogue	En-tête :
CSCvx74133	Instance d'application s'affiche comme démarrée au lieu d'en ligne
CSCvy51481	[ENH] FTD devrait afficher une erreur ou un avertissement lors de l'association d'un certificat non valide à l'interface pour le VPN
CSCvz59859	Description de la défaillance F1758 ne doit pas être spécifiques aux sous-interfaces
CSCvz70310	L'ASA peut ne pas créer la règle NAT pour SNMP avec : « erreur NAT impossible de réserver des ports ».
CSCwa82791	Amélioration : Prise en charge des instantanés des files d'attente RX sur les interfaces InternalData lorsque « Blocks free curr » (Bloquer le courant libre) est faible
CSCwb02701	FXOS ne relance pas la synchronisation NTP avec les serveurs
CSCwb02741	État de synchronisation de l'heure et message erreur ne donnent aucun détail sur le rejet du serveur NTP
CSCwb03293	Débogage IKEv2 : les politiques reçues et les politiques attendues sont vides
CSCwc01843	Pour la haute disponibilité ou la grappe FTD, un nom de périphérique incorrect peut s'afficher dans les statistiques de l'interface utilisateur et du tableau de bord
CSCwd65732	La carte netmod 2X100G affiche 10 Mbit/s sur le premier membre du canal de port lors de l'ajout de la deuxième interface
CSCwd67100	Recherche de la source et rechargement d'ASA sur le processus Datapath

ID du bogue	En-tête :
CSCwe02012	ASA/FTD peut rechercher la source et recharger dans le nom de fil « lina »
CSCwe18462	ASA/FTD : Amélioration de la journalisation de l'inspection GTP
CSCwe18467	ASA/FTD : Validité du moteur d'inspection GTP
CSCwe21884	Rédaction d'enveloppe autour de la commande « kill » pour journaliser qui l'appelle
CSCwe34826	L'utilisateur de prévention des intrusions n'est pas en mesure de modifier l'action de prévention des intrusions et la politique de fichiers
CSCwe82107	Alerte d'intégrité pour [FSM:STAGE:FAILED] : configuration du serveur avec protocole AAA (authentication, authorization and accounting) externe
CSCwf16001	L'implémentation du partage secret de Shamir par HashiCorp Vault utilisait des précalculs.
CSCwf27337	KP : nettoyage/reformatage du deuxième disque (MSP) lors de la réinstallation de Cisco FTD
CSCwf39108	Les boucles de pare-feu peuvent se bloquer et entraîner une perte de paquets lorsque l'équilibreur de charge asp par paquet automatique est utilisé
CSCwf64429	Impossible de charger l'image de la version FTD dans le FCM
CSCwf69880	Recherche de la source et rechargement du pare-feu en raison du fil SNMP
CSCwf70275	FTD : L'identité du serveur TLS ne fonctionne pas si la taille du client Hello est supérieure aux octets TCP MSS
CSCwf75694	ASA – L'inspection GTP a abandonné le message « Supprimer la réponse au contexte PDP » en raison d'un TEID=0 non valide
CSCwf77994	Fausses alertes de processeur élevé critique pour les cœurs du système d'appareils FTD exécutant une utilisation élevée instantanée
CSCwf84318	Recherche de la source ASA/FTD et rechargement sur le fil DATAPATH
CSCwf99434	Échec de transfert du nouveau fichier image vers FPR2130 et recherche de la source observée
CSCwh09968	ASA/FTD : Recherche de la source et rechargement en raison d'une modification de la NAT et de l'utilisation du DVTI
CSCwh10931	Recherche de la source ASA/FTD et rechargement lors de l'appel de la commande CLI « show webvpn saml idp »
CSCwh13040	Déroutement incomplet. snmpwalk sur 816 MIB obtient un délai d'expiration
CSCwh14475	Les événements FTD ont cessé d'être envoyés à FMC, journaux du gestionnaire d'événements « publication bloquée »

ID du bogue	En-tête :
CSCwh19475	Le flux intermittent est mis sur liste blanche par le SNORT pour le trafic d'ID d'application inconnu.
CSCwh19613	Appareils de sécurité adaptables Cisco ont planté avec scénarios Saml
CSCwh27886	Gestionnaire de châssis affiche l'erreur du serveur interne HTTP 500 dans des cas spécifiques
CSCwh28218	Journal système non mis à jour lorsque le nom de la règle de préfiltre est modifié
CSCwh29276	ASA : Recherche de la source et rechargement lors du passage du mode unique au mode multiple
CSCwh40294	Recherche de la source ASA en raison d'un événement d'urgence lors de la configuration SNMP
CSCwh43230	Licence de cryptage renforcé non appliquée aux pare-feux des appareils de sécurité adaptables Cisco dans HA
CSCwh45450	2100 : Interfaces manquantes dans FTD après la suppression d'interfaces en tant que membres d'un canal de port
CSCwh45935	Cœur Lina observé dans la version 6.4.0.17-22 en Kp avec trafic évolutif
CSCwh48776	Problème découvert dans Python avant la version 3.8.18, 3.9.x avant la version 3.9.18,
CSCwh51872	Le message asa_log_client est sorti 1 fois et a été vu plusieurs fois
CSCwh52710	evaluate open-vm-tools / VMware Tools on FMC for VMware -- CVE-2023-20900 and VMSA-2023-0019 (évaluer open-vm-tools / VMware Tools sur FMC pour VMware : CVE-2023-20900 et VMSA-2023-0019)
CSCwh57814	Le package html/template n'applique pas les règles appropriées pour gérer o
CSCwh60971	Le regroupement NAT ne fonctionne pas correctement, bien qu'il n'atteigne pas la limite d'ID d'objet de 32 k.
CSCwh62080	additional command outputs needed in FTD troubleshoot for blocks and ssl cache (sorties de commande supplémentaires nécessaires dans le dépannage de FTD pour les blocs et le cache SSL)
CSCwh63211	Cœur Lina au niveau de snp_nat_xlate_verify_magic.part et traces logicielles
CSCwh68068	L'identifiant du routeur Firepower WCCP change aléatoirement lorsque les VRF sont configurés
CSCwh69156	FTD-HA ne bascule pas parfois lorsque SNORT3 se bloque
CSCwh69843	WM DT – L'appareil de sécurité adaptable en mode transparent n'envoie pas les mêmes paquets d'annonce de routeur IPv6 à tous les nœuds
CSCwh71262	Faible trouvée dans glibc. Dans une situation peu courante, la commande gaih_inet

ID du bogue	En-tête :
CSCwh72070	Le rechargement prend une éternité lorsque la commande de rechargement est émise à l'invite lina lorsque les périphériques sont en mode haute disponibilité
CSCwh78118	Recherche de la source ASA/FTD et rechargement sur le processus fsm_send_config_info_initiator
CSCwh81366	Deuxième disque dur [Multi-Instance] (FPR-MSP-SSD) non utilisé
CSCwh83517	Le tunnel VTI tombe en panne en raison d'un changement de route détecté dans le scénario VRF
CSCwh91065	Recherche de la source Lina : nom du fil : DATAPATH lors de la fin de la session
CSCwh92345	Fichier crypto_archive généré après la mise à niveau logicielle.
CSCwh94029	Faible trouvée dans le sous-système Netfilter, dans le noyau Linux Le n
CSCwh94116	Faible trouvée dans le sous-système Netfilter, dans le noyau Linux Le x
CSCwh94193	urllib3 est une bibliothèque cliente HTTP conviviale pour Python. urllib3 doe
CSCwh95025	Les connexions GTP, dans certaines circonstances, ne sont pas effacées lors de l'émission d'une clear conn.
CSCwh95277	Recherche de la source FTD en raison d'un épuisement de la mémoire du système
CSCwh95443	Déversement du chemin de données, ce qui entraîne l'exclusion des unités de mise en grappe de la grappe
CSCwh96055	Les serveurs DNS de gestion peuvent être inaccessibles si l'interface de données est utilisée comme passerelle
CSCwh99398	ASA/FTD peut rechercher la source et recharger dans le nom de fil « DATAPATH-34-17852 »
CSCwi00713	Défaut de fuite de mémoire trouvé dans l'utilitaire tiffcrop de Libtiff. Ce problème
CSCwi01323	Protocoles SNMP OID ifOutDiscards sur MIO ont toujours une valeur nulle alors que l'affichage de l'interface d'affichage a une valeur autre que zéro
CSCwi02754	Redémarrage soudain en veille de FTD 1120
CSCwi03407	Recherche de la source sur FP2140 sans point de déclenchement.
CSCwi04351	Échec de mise à mise à niveau de FTD dans script 999_finish/999_zz_install_bundle.sh
CSCwi05240	ASA – Recherche de la source pour le périphérique en veille pendant la synchronisation de l'ACL-DAP
CSCwi06797	Recherche de la source ASA/FTD et rechargement sur le fil DATAPATH
CSCwi20045	ASA/FTD peut effectuer une recherche de la source et un rechargement dans le nom de fil « lina » en raison d'un chien de garde dans le code 9.16.3.23

ID du bogue	En-tête :
CSCwi23964	Python 3.x à 3.10 présente une vulnérabilité de redirection ouverte dans lib/h
CSCwi24007	Problème découvert dans le noyau Linux des versions antérieures à 6.3.3. Il existe un
CSCwi24116	Twisted est un cadre basé sur les événements pour les applications Internet Antérieur à
CSCwi31480	Alerte : échec de désactivation, raison : l'erreur interne n'est pas effacée du FCM ou de l'interface de ligne de commande après l'accusé de réception
CSCwi31558	Les journaux d'extraction de fichier ne sont pas reconnus par le gestionnaire de disques, ce qui entraîne un espace disque élevé
CSCwi31966	Les débogages de FTD ADI peuvent afficher un server_group et/ou un realm_id incorrect pour les sessions authentifiées par SAML
CSCwi36244	Dans versions BuC Traceroute 2.0.12 à 2.1.2 avant 2.1.3, le certificat d'encapsulation
CSCwi36311	Utilise la fonction d'arrêt (kill Tree) dans SMA au lieu de SIGTERM
CSCwi36843	Journalisation détaillée liée à la raison du changement d'état administratif de la sous-interface pendant les opérations
CSCwi38662	La haute disponibilité de FTD ne doit pas être créée partiellement sur FMC
CSCwi40193	Bouclage du trafic DCE/RPC pendant la recherche sous-optimale
CSCwi40302	Le déploiement échoue sur le nouvel appareil AWS FTDv avec « no username admin »
CSCwi43492	Recherche de la source ASA et rechargement sur le nom de fil : DATAPATH
CSCwi44208	Faible mémoire/stress entraînant une recherche de la source dans SNMP
CSCwi44912	Recherche de la source ISA3000 et recharge de la boucle de démarrage
CSCwi45878	ASA/FTD : L'équilibrage de charge DNS avec SAML ne fonctionne pas avec l'équilibrage de charge VPN
CSCwi48699	Recherche de la source ASA et rechargement sur le nom de fil : pix_flash_config_thread
CSCwi49770	Rechargement de la source ASA/FTD et recharger dans le nom de fil « Datapath »
CSCwi49884	TCP MSS est remplacé par la valeur par défaut lors de la création d'une interface VTI ou de boucle avec retour
CSCwi52008	Recherche de la source Snort3 et redémarrage avec conditions de concurrence
CSCwi53949	Recherche de la source Snot3 dans TcpReassembler::scan_data_post_ack
CSCwi53987	Paramètres du protocole SSL ne modifient pas la configuration du certificat de l'interface graphique FDM et ne désactivent pas TLSv1.1
CSCwi55938	L'utilisation de la commande « show asp drop » nécessite de meilleures mises à jour pour les abandons liés à la grappe

ID du bogue	En-tête :
CSCwi56499	La fonction de mandataire direct crée des pointes dans le processeur du CP avec un flux de trafic non authentifié
CSCwi56667	Recherche de la source ASA et rechargement du nom de fil « fover_parse » en mode veille après la modification du groupe de basculement
CSCwi56743	Paramètre de quota MSP incorrect pour les instances
CSCwi57670	RAVPN SAML : Le navigateur externe envoie un message erreur lorsque FTD/ASA ne parvient pas à analyser l'assertion
CSCwi59271	Suppression du journal système « End of script output before headers » (fin de la sortie du script avant les en-têtes) dans FXOS
CSCwi60285	ASA/FTD peut rechercher la source et recharger dans le nom de fil « lina »
CSCwi61135	Échec de l'activation des débogues sur la session SSH
CSCwi62796	Recherche de la source ASA/FTD et rechargement liés au traitement du trafic SSL/DTLS
CSCwi63743	ASA/FTD peut effectuer une recherche de la source et être rechargé dans le nom de fil « appAgent_monitor_nd_thread » et RIP : _lina_assert.
CSCwi64829	recherche de la source et rechargement autour de la fonction à haute disponibilité
CSCwi65116	DHCPv6 : Recherche de la source ASA sur le nom du fil : CLIENT DHCPv6
CSCwi66461	Message WARN (vitesse non compatible, suspendu) lors de la création d'un port-channel sur Victoria CE
CSCwi66676	ASA/FTD peut rechercher la source et se recharger dans le nom de fil « webvpn_task »
CSCwi68833	ASA/FTD : fuite de mémoire causée par le basculement qui ne libère pas le cache de clés dnscrypt en raison d'un flux parapluie non synchronisé
CSCwi69091	ASA/FTD peut rechercher la source et recharger dans le nom de fil « lina »
CSCwi70492	Le pare-feu présente une erreur de synchronisation d'application en mode pseudo-veille et utilise les adresses IP de l'unité active
CSCwi71998	« Stream : erreur de normalisation TCP dans NO_TIMESTAMP » s'affiche lorsque la politique SSL déchiffrer tout est utilisée
CSCwi72294	FTD : améliorer ou optimiser la logique de vérification des paquets LSP pour l'exécuter plus rapidement
CSCwi74214	Recherche de la source ASA/FTD et rechargement dans le nom du fil : daemon IKEv2 lors du passage de la haute disponibilité active à la haute disponibilité en veille
CSCwi75198	FTD en veille faisant l'objet d'une recherche de source et d'un rechargement périodiques

ID du bogue	En-tête :
CSCwi75967	CCM ID 62 - LTS18
CSCwi76361	Le filtre MAC de pare-feu transparent ne capture pas les trames avec la version MAC dst STP-UplinkFast de manière cohérente
CSCwi78191	Problème découvert dans drivers/input/input.c dans le noyau Linux b
CSCwi78193	Problème découvert dans le noyau Linux des versions antérieures à 6.6.8. do_vcc_ioctl
CSCwi78200	Vulnérabilité trouvée dans GnuTLS. Les temps de réponse aux fichiers c malformés
CSCwi78206	Vulnérabilité trouvée dans GnuTLS, où un poste de commande (qui utilise gnuTL
CSCwi78370	41xx/93xx : mise à jour CiscoSSH (gestionnaire de châssis FXOS) pour l'adresse CVE-2023-48795
CSCwi79037	Les services clients IKEv2 ne sont pas activés - le profil XML n'est pas téléchargé
CSCwi79042	Recherche de la source FTD/Lina et rechargement des paires à haute disponibilité, dans le chemin de données, après l'ajout de la politique NAT
CSCwi79120	Certaines sessions SSH n'expirent pas, ce qui empêche ssh et la console de se connecter à la CLI de FXOS
CSCwi79393	Le déploiement de la politique échoue lors de la suppression de la politique DNS Umbrella de Security Intelligence
CSCwi80979	Snort supprime les informations de paquet et injecte son paquet avec des données de 0 octet
CSCwi81503	La détection HTTP/HTTPS pour l'application doit échouer plus tôt
CSCwi81771	Impossible d'envoyer la disposition du fichier inconnu à ThreatGrid en raison d'un problème de cache Mem
CSCwi83890	Le fichier de rapport généré pour la politique AC est vide
CSCwi84314	L'interface de ligne de commande de l'ASA se bloque avec « show run » sur plusieurs SSH
CSCwi84615	Certains journaux stdout non soumis à la rotation par logrotate
CSCwi85689	Identifier le serveur TLS : la sortie de « show asp table socket » affiche plusieurs entrées TLS_TRK
CSCwi85951	Faillie de sortie d'urgence trouvée dans __ext4_remount dans fs/ext4/super
CSCwi85953	Dans rds_rcv_track_latency dans net/rds/af_rds.c dans le noyau Linux
CSCwi87382	Recherche de la source et rechargement sur l'unité principale lors de l'exécution des débogages sur la session SSH
CSCwi90571	Accès à un site Web par le biais d'échecs du VPN SSL sans client

ID du bogue	En-tête :
CSCwi90751	FTD/ASA – Les requêtes SNMP utilisant snmpwalk n'affichent pas toutes les interfaces « nameif »
CSCwi90998	Échec de l'interrogation SNMP ASA pour la MIB FXOS DME environnementale (.1.3.6.1.4.1.9.9.826.2)
CSCwi92875	Vérifier la taille du cache des métadonnées lors de la génération d'événements rétrospectifs
CSCwi92924	Problème de fuite de mémoire trouvé dans ctnetlien_creer_connTrack dans net/n
CSCwi92927	Vulnérabilité de cycle d'utilisation après interruption de service dans le netfilter, dans le noyau Linux : nf_table
CSCwi92930	linux-pam (alias Linux PAM) avant la version 1.6.0 permet aux agresseurs de créer un
CSCwi92932	copy_params dans rivers/md/dm-ioct.c dans le noyau Linux jusqu'à la version 6.7.1
CSCwi95228	« crypto ikev2 limit queue sa_init » est réinitialisé après le redémarrage
CSCwi95796	FTD SNMP OID 1.3.6.1.4.1.9.9.109.1.1.1.1.7 renvoie toujours 0 % pour la moyenne SysProc
CSCwi95994	Les navigateurs basés sur Chromium ont des conflits de connexion SSL lorsque FIPS CC est activé sur le pare-feu.
CSCwi97836	Recherche de la source et rechargement de l'appareil de sécurité adaptable après la configuration de la capture sur nlp_int_tap et la suppression du contexte
CSCwi97839	Validation de recherche de la source FTD dans vni_idb_get_mode et rechargée
CSCwi98274	Décompresser la version 5.52 date de 2005 et contient plusieurs vulnérabilités
CSCwi99429	Échec du déploiement de la politique de restauration n'a pas reconfiguré les appareils FTD
CSCwj00956	Processus Snort inondant les messages syslog-ng, ce qui entraîne la suppression de notre journal système syslog-ng sur la plateforme KP
CSCwj02505	Recherche de la source des Checkheaps par l'appareil de sécurité adaptable lors de la saisie du même ID de moteur deux fois
CSCwj03764	Dans le cas d'un ISP double à rayons, si ISP2 est en panne, les tunnels VTI liés à ISP1 oscillent.
CSCwj05151	ASA/FTD peut effectuer une recherche de la source et recharger dans le nom de fil « DATAPATH » en raison d'une assertion de verrouillage GTP
CSCwj05484	Mise à niveau de l'appareil de sécurité adaptable de la version 9.16 à la version 9.18 entraînant une modification des valeurs d'attribut LDAP par l'ajout d'une barre oblique « \ »

ID du bogue	En-tête :
CSCwj08021	Code d'analyse du message DNS dans « named » comprend une section dont
CSCwj08023	Certains aspects DNSSEC du protocole DNS (dans RFC 4033, 4034, 4035, 6
CSCwj08030	libexpat jusqu'à la version 2.5.0 permet un événement de déni de service par consommation de ressources
CSCwj08031	libexpat jusqu'à la version 2.5.0 permet l'expansion récursive d'entité XML si XML_DT
CSCwj08066	Déni de service vulnérabilité en raison d'un blocage trouvé dans sctp_
CSCwj08083	Problème découvert dans libxml2 versions précédant 2.11.7 et 2.12.x, version précédant 2.1
CSCwj08153	Faible de mémoire saturée trouvée dans libtiff qui pourrait être déclenchée par
CSCwj08667	Recherche de la source ASA/FTD et rechargement lors de l'établissement de la session SSL
CSCwj09110	Le chargement de fichiers par le biais du portail sans client ne fonctionne pas comme prévu après la mise à niveau de l'appareil de sécurité adaptable
CSCwj09999	Modification l'unité de transfert maximale du FP 3100 sur interface de gestion ne persiste PAS pendant les redémarrages (le retour à l'unité de transfert par défaut)
CSCwj10451	Le périphérique secondaire a redémarré lors du redémarrage du périphérique principal.
CSCwj12131	Échec de basculement lorsque lina_io_write échoue avec l'erreur EPIPE
CSCwj12173	Le fil de nettoyage du cache des politiques doit nettoyer tout cache laissé ouvert pour une session déconnectée
CSCwj12924	Faible trouvée dans le sous-système Netfilter, dans le noyau Linux Le i
CSCwj13910	Sortie du SA de chiffrement IPsec ne présentant aucune erreur SA avec le déchargement IPsec activé
CSCwj14028	CCM ID 67 - LTS18
CSCwj14624	La sauvegarde se termine avec une erreur d'allocation de mémoire sur 4115
CSCwj14832	SAML : Un échec de vérification du jeton AnyConnect de connexion unique est observé après une authentification réussie
CSCwj14927	Cisco FTD : le serveur principal joue un rôle actif après le rechargement
CSCwj15125	ASA/FTD peut effectuer une recherche de la source et un rechargement dans le nom de fil « lina » lié à l'infrastructure de la minuterie Netflow
CSCwj17447	ASA/FTD peut effectuer une recherche de la source et un rechargement dans le nom de fil « DATAPATH-6-26174 »
CSCwj19653	FTD – Recherche de la source et rechargement en raison d'une NAT impliquant des objets fqdn

ID du bogue	En-tête :
CSCwj20067	ASA : Les messages d'avertissement ne s'affichent pas lorsque la NAT de l'interface statique est configurée
CSCwj21880	FTD avec l'optimisation des objets d'interface activée bloque le trafic après le changement de nom des noms de zone
CSCwj22086	L'unité active passe à l'état désactivé en cas d'incompatibilité en mode de pare-feu
CSCwj22235	Recherche de la source sur lina et rechargement en raison de mps_hash_memory pointant vers une table de hachage nulle
CSCwj22990	Après la mise à niveau de l'appareil de sécurité adaptable, « Slot 1: ATA Compact Flash memory » affiche une valeur différente
CSCwj23192	La vérification supplémentaire des fichiers n'est pas signalée avec la commande pmttool SecureLSP lsp-rel-xxx
CSCwj24828	Problème lorsque deux objets FQDN avec la même adresse IP sont ajoutés dans la source ou la destination (FTD/ASA)
CSCwj25975	FTD/ASA : La génération d'un CSR avec une virgule entre l'attribut « Nom de l'entreprise » ne fonctionne pas comme prévu
CSCwj28153	Lina contient du code source libexpat obsolète
CSCwj28437	Snort3 : Échec du trafic SQL après la mise à niveau en raison de numéros de séquence non valides et d'accusés de réception non valides
CSCwj30825	Fuite de mémoire dans SFDataCorrelator après la désinscription d'un appareil actif
CSCwj30980	Ajout de débogages et d'une commande show pour capturer l'utilisation de l'ID dans le flux SXP CTS.
CSCwj31918	Défaillance de segmentation avec « logger_msg_dispatch » lors de la synchronisation à haute disponibilité
CSCwj32035	Les utilisateurs VPN sans client ne peuvent pas accéder aux pages avec l'authentification de base HTTP
CSCwj33487	L'ASA/FTD peut effectuer une recherche de la source et se recharger pendant le traitement du trafic DTLS
CSCwj33580	Les tunnels IKEv2 fluctuent en raison de la fragmentation et de la limitation causées par plusieurs chiffrements/propositions.
CSCwj33891	Épuisement de la mémoire de grappe ASA/FTD causé par le processus NAT lors de la publication des allocations de blocs de port
CSCwj34881	La commande pour afficher les compteurs pour la politique d'accès filtrée avec une adresse IP source donne un résultat incorrect
CSCwj34975	Plusieurs interfaces de contexte ne parviennent pas à transmettre le trafic

ID du bogue	En-tête :
CSCwj35701	Connexion prématurée de la protection DNS en raison d'une condition de synchronisation
CSCwj38871	Recherche de la source ASA avec nom de fil SSH
CSCwj38928	Latence élevée observée sur FPR31xx ou FPR42xx
CSCwj39107	Croissance de la mémoire SFDDataCorrelator lors du nettoyage d'un nombre élevé d'anciennes identités de service
CSCwj40597	FTD : Les sauvegardes échouent en mode multi-instances ou autonomes avec l'erreur « La sauvegarde est survenue de manière inattendue »
CSCwj40665	Suivi supplémentaire de la mémoire dans SFDDataCorrelator
CSCwj40761	ASA/FTD peut effectuer une recherche de la source dans le nom de fil : **gestionnaire de statistiques CTM KC FPGA**
CSCwj43345	L'interrogation SNMP pour certains OID peut entraîner des sauts de CPU et une latence élevée peut être observée pour les paquets ICMP
CSCwj43355	Bogue dans QEMU pouvant entraîner une opération I/O pour invité autrement adressée à
CSCwj43379	libexpat jusqu'à la version 2.6.1 permet une attaque par expansion d'entité XML lorsque
CSCwj43466	Vulnérabilité de débordement de la mémoire tampon trouvée dans LibTIFF, dans extractI
CSCwj44398	lors de la définition de la carte de routage dans la route RIP sur FTD, la mise à jour des routes ne fonctionne pas après le redémarrage de FTD
CSCwj45822	Cisco Secure Client incapable d'effectuer la connexion. Le poste de travail de Cisco Secure n'est pas installé sur le client
CSCwj48704	Recherche de la source et rechargement de l'appareil de sécurité adaptable lors de l'accès au système de fichiers à partir d'ASDM
CSCwj48754	Utilisation élevée de la mémoire SFDDataCorrelator lors du redémarrage avec de grands hôtes de carte de réseau
CSCwj49958	Échec de négociation du cryptage IPSEC à « Failed to compute a hash value » (échec du calcul de la valeur de hachage)
CSCwj50406	Toutes les routes BGP IPV6 configurées dans le périphérique fluctuent
CSCwj53725	Recherche de la source observée lors de l'application de « aucun basculement » et « basculement » dans l'appareil de sécurité adaptable de secours
CSCwj55036	ASA/FTD : Un retard dans une commande crypto asynchrone entraîne une recherche de la source puis un rechargement.

ID du bogue	En-tête :
CSCwj59861	ASA/FTD peut effectuer une recherche de la source et se recharger dans le nom de fil « lina » en raison du processus SCP/SSH
CSCwj60265	ASA/FTD peut effectuer une recherche de la source et se recharger dans le nom de fil « DATAPATH-1-16803 »
CSCwj61885	Fuite du descripteur de fichier lors de la validation des images de mise à niveau
CSCwj62723	Message d'erreur envoyé vers la console sur les appareils Firepower 2100 lors de l'activation de la configuration SSH
CSCwj62984	Snort3 : Trafic de requête MSSQL corrompu par la gestion du chevauchement de stream_tcp entraînant SQL HY000
CSCwj68096	Accès à la console bloqué pour l'ASAv hébergé dans le CSP après la mise à niveau vers la version 9.18.3.56
CSCwj68385	Recherche de la source et rechargement continu Snort3 avec chaque déploiement
CSCwj68783	Configurations FTD/ASA-HA non synchronisées, car le processus de synchronisation des commandes envoie des configurations avec des caractères spéciaux
CSCwj69632	SHA1 est l'algorithme de hachage par défaut pour le certificat du Firepower Chassis Manager sur 4110
CSCwj72022	Augmentation du temps de déploiement de 30 à 45 secondes après la mise à niveau lors de l'application d'un paramètre de plateforme spécifique
CSCwj72369	L'appel de synchronisation s'est bloqué, ce qui a entraîné une boucle de démarrage
CSCwj72683	ASA – Les signets sur le portail WebVPN ne sont pas accessibles après une connexion réussie.
CSCwj73053	L'appareil de sécurité adaptable peut rechercher la source et recharger dans le nom de fil « DATAPATH-21-16432 »
CSCwj73061	OID SNMP pour CPUPercentTotal1min omet les entrées de cœurs de CPU Snort lors de l'interrogation
CSCwj74323	Fuite de mémoire ASAv impliquant PKI/chiffrement pour VPN
CSCwj76503	Les journaux système continuent d'être envoyés après la désactivation de la classe de journalisation sur l'appareil de sécurité adaptable
CSCwj81743	FTD – Recherche de la source et rechargement en raison d'une NAT impliquant des objets fqdn
CSCwj82285	ASA/FTD peut rechercher la source et recharger dans le nom de fil « sdi_work »
CSCwj82736	Échec de l'établissement de liaison TLS si un paquet Hello du client fragmenté est reçu en panne

ID du bogue	En-tête :
CSCwj82903	Le déploiement de FDM à haute disponibilité échoue avec l'erreur « ApplicationException : impossible d'exporter vers la base de données »
CSCwj83185	FTD/ASA : Recherche de la source FTD en veille et rechargement après activation du suivi de la mémoire
CSCwj83634	Affichage du message « reg_fover_nlp_sessions : échec du basculement ioctl C_FOREG »
CSCwj85106	FMC lors de la mise à niveau entraîne la perte de FTDv de son niveau de performance
CSCwj85333	FPR peut abandonner les connexions TLS1.3 lorsque le chiffrement kyber hybride est activé dans le navigateur Web
CSCwj86527	Interruptions SNMP v1 et v2c de diagnostic et de données cessent de fonctionner sur un KP/vFTD après la mise à niveau du produit
CSCwj87501	ASA/FTD peut rechercher la source et recharger dans le nom de fil « fover_FSM_thread »
CSCwj88400	FTD peut effectuer une recherche de la source et recharger le nom de processus lina lors du traitement de la réponse msg appAgent
CSCwj89050	Validation d'entrée défectueuse dans Apache permet aux attaques ou
CSCwj89051	Dans GNU tar avant la version 1.35, attributs d'extension mal gérés dans une archive PAX
CSCwj89054	Agresseur qui peut forcer un terminal HTTP/2 à lire des quantités quelconques de
CSCwj89264	FTD HA : Recherche de la source et rechargement dans netsnmp_oid_compare_ll
CSCwj89315	Fractionnement de la réponse HTTP en plusieurs modules dans l'allocation du serveur HTTP Apache
CSCwj89402	Vulnérabilité suivante résolue dans le noyau Linux : n
CSCwj89404	Vulnérabilité suivante résolue dans le noyau Linux : b
CSCwj89406	Vulnérabilité suivante résolue dans le noyau Linux : b
CSCwj89417	Vulnérabilité suivante résolue dans le noyau Linux : d
CSCwj89425	Vulnérabilité suivante résolue dans le noyau Linux : B
CSCwj89432	Les en-têtes entrants HTTP/2 dépassant la limite sont temporairement mis en mémoire tampon i
CSCwj89434	mur dans util-linux jusqu'à la version 2.40, souvent installée avec setgid tty permi
CSCwj89445	La fonction iconv () de la bibliothèque C GNU versions 2.39 et antérieures peut
CSCwj89447	inférieur à 653 permet d'exécuter des commandes de système d'exploitation avec un caractère de retour à la ligne i

ID du bogue	En-tête :
CSCwj90826	Échec du déchiffrement SSL Snort2 avec clé connue sur Chrome v124 et versions ultérieures.
CSCwj93921	L'appareil de sécurité adaptable après la mise à niveau vers la version 9.18.4.24 n'a pas pu enregistrer la configuration avec l'erreur suivante : « Configuration ligne trop longue »
CSCwj95322	disable stat check for file (désactiver la vérification des statistiques pour le fichier)
CSCwj95590	Le navigateur redirige vers la page de connexion lorsque l'utilisateur clique sur le signet WebVPN
CSCwk00604	L'appareil de sécurité adaptable ne parvient pas à lancer l'authentification AAA avec IKEv2-EAP et le client VPN natif Windows
CSCwk02332	Snort2 – Échec du déchiffrement SSL et certains sites Web ne se chargent pas sur Chrome v124 et versions ultérieures
CSCwk02804	Connexions WebVPN bloquées à l'état CLOSEWAIT
CSCwk02928	ASA/FTD peut rechercher la source et recharger dans le nom de fil « PTHREAD »
CSCwk04290	FPR 21xx – Recherche de la source dans le nom du processus : lina-mps pendant le fonctionnement normal
CSCwk04492	L'interface de ligne de commande de l'appareil de sécurité adaptable se bloque avec « show run » (afficher l'exécution) avec plusieurs sessions SSH
CSCwk05800	Échec de l'interrogation SNMP ASA/FTD en raison d'un chevauchement de réseaux dans le groupe d'hôtes snmp-server
CSCwk05826	nsd : débordement du tampon basé sur la pile dans le cache du groupe réseau si le nom
CSCwk05828	nsd : cache du groupe réseau peut mettre fin au démon en cas d'échec d'allocation de mémoire
CSCwk05851	Ligne « set ip next-hop » supprimée de la configuration lors du rechargement si l'adresse IP correspond à un NAME
CSCwk06564	Ajouter un nouveau journal système pour les routes pour l'ajout/suppression de NP
CSCwk06573	Serviceabilité : Amélioration du routage des débogues infra et ajout d'un nouveau pour les conditions d'erreur
CSCwk07934	Le biais de l'horloge entre FXOS et Lina entraîne un échec du traitement de l'assertion SAML
CSCwk08241	FTD ne résout pas le FQDN pour les ACLs par intermittence
CSCwk08476	Recherche de la source FTD/ASA et rechargement en raison d'une fuite de mémoire « show bgp summary »

ID du bogue	En-tête :
CSCwk08576	command to print the debug menu setting of service worker (commande pour imprimer les paramètres du menu de débogage de Service Worker)
CSCwk10884	Défaillance de connectivité en raison d'une incompatibilité entre l2_table et l'adresse mac de la sous-interface
CSCwk11983	UC LINA élevé observé en raison de NetFlow en raison de la configuration « (Exportation et transfert retarder la création de flux) »
CSCwk12497	Recherche de la source et rechargement sur l'unité active en raison d'une opération d'interruption de la haute disponibilité.
CSCwk12673	Session TCP interrompue si Keep-Alive avec 1 octet est reçu
CSCwk12698	Sondages SNMP de l'interface de gestion de contexte d'administration ne parvient pas à afficher toutes les interfaces dans tous les contextes
CSCwk13631	Recherche de la source et rechargement pendant la mise à niveau de FTD en raison de la NAT de l'objet réseau FQDN
CSCwk13812	ASA/FTD transfère incorrectement l'attribut de communauté étendue après la mise à niveau
CSCwk14685	Cisco FTD : Interface de gestion ne fonctionne pas, bien qu'elle soit opérationnelle
CSCwk14909	Perte du trafic avec « règle-transaction-en-cours » après un basculement avec TCM cfgd en mode multi-ctx
CSCwk17637	La liaison d'état arrête d'envoyer des messages Hello après le basculement déclenché par la recherche de la source Snort dans FTD à haute disponibilité
CSCwk17854	FTD n'envoie pas de requête de type A après avoir reçu une erreur de refus d'un serveur DNS dans la requête AAAA.
CSCwk20823	UC Snort3 élevée, car le trafic chiffré n'est pas autorisé lorsque TSID est activé
CSCwk20882	Numéro de séquence ESP de 0 envoyé après l'établissement ou le renouvellement de la SA
CSCwk21561	Ajouter un message d'avertissement lors de la configuration de l'unité CCL MTU
CSCwk22034	Snmpwalk affiche des vitesses d'interface incorrectes pour des valeurs supérieures ou égales à 10 G
CSCwk22574	Retirer les trames/les paquets SGT pour permettre le déchiffrement VTI
CSCwk22759	Problème lié à la définition de certains fuseaux horaires (p. ex. GMT+1) sur Cisco ASA Firepower en mode appareil
CSCwk22993	Vulnérabilité suivante résolue dans le noyau Linux : t
CSCwk24176	FTD/ASA – Le trafic VPN circulant dans le périphérique peut déclencher des recherches de recherche et des rechargements.

ID du bogue	En-tête :
CSCwk25117	Amélioration : Ajout de la prise en charge des applications pour bloquer les défaillances AAA consécutives sur LINA
CSCwk25755	Vulnérabilité suivante résolue dans le noyau Linux : n
CSCwk25756	Requests est une bibliothèque HTTP. Avant la version 2.32.0, lorsque des demandes sont effectuées au moyen de
CSCwk25759	Vulnérabilité suivante résolue dans le noyau Linux : B
CSCwk25761	Vulnérabilité suivante résolue dans le noyau Linux : b
CSCwk25762	Vulnérabilité suivante résolue dans le noyau Linux : i
CSCwk25764	Vulnérabilité suivante résolue dans le noyau Linux : H
CSCwk26968	La fonctionnalité de sauvegarde ne sauvegarde pas/restaure la configuration DAP en mode contexte multiple.
CSCwk27175	ASA/FTD : Augmentation considérable du temps nécessaire au chargement de la configuration
CSCwk27830	ASA/FTD peut rechercher la source et recharger dans le nom de fil « lina »
CSCwk27965	Safety Net pour les plantages de récursivité infinie en raison d'un mauvais état TCP de flux en mode Post-ACK
CSCwk31371	NAT_HARDEN : CGNAT se rompt lorsque le mappage ifc est configuré comme tout
CSCwk32501	Processus d'épuisement du bloc 256/1550 fover_thread
CSCwk35710	FTD/lina peut effectuer une recherche de la source et se recharger lorsque la commande « show capture » est exécutée dans le script EEM
CSCwk36312	Utilisation élevée du processeur lors de l'« épuisement du bloc de mise à jour » entraînant l'arrêt du BGP flap sur FTD
CSCwk39974	L'état d'enregistrement d'Umbrella n'est pas synchronisé avec les nœuds de données nouvellement ajoutés
CSCwk40726	Appels d'API REST de FMC pour obtenir les données de politique de CA expirent, lenteur de l'interface graphique de politique de CA avec requête de règle plus volumineuse
CSCwk41065	Page sur les mises à niveau de produit affichant « Unknown Family 66 » pour les paquets de mise à niveau de FMC
CSCwk44245	Vulnérabilité suivante résolue dans le noyau Linux : i
CSCwk44246	Vulnérabilité suivante résolue dans le noyau Linux : i
CSCwk45975	La configuration de déchiffrement TLS1.3 sur la politique SSL affecte le trafic DND.

ID du bogue	En-tête :
CSCwk48975	La sortie du traceur de paquets ajoute incorrectement « control-plane » aux abandons pour le groupe d'accès au plan de données
CSCwk50044	Aucune des méthodes Is (IsPrivate, IsLoopback, etc.) indiquées ne fonctionne normalement
CSCwk50055	url.c dans GNU Wget jusqu'à 1.24.5 traite mal les points-virgules dans les informations utilisateur
CSCwk56388	Le trafic GRE est abandonné après le basculement
CSCwk56443	Appels d'API d'adresses de réseau prenant beaucoup de temps
CSCwk57933	Vulnérabilités dans le noyau Linux CVE-2023-52439
CSCwk57949	Vulnérabilités dans le noyau Linux CVE-2023-52435
CSCwk59458	21xx : blocages du processus de débogage qui empêchent la récupération des opérations d'écriture bloquées
CSCwk61157	Recherche de la source FTD LINA et rechargement du fil dhcp_daemon
CSCwk62297	Évaluation du protocole ssp pour la vulnérabilité regreSSHion dans OpenSSH
CSCwk62381	L'ASA peut effectuer une recherche de la source et un rechargement parce que ssh/client a atteint un pointeur nul lors de l'utilisation du protocole SCP.
CSCwk63733	Les interfaces surveillées par HA passent à l'état « En attente », puis à l'état « Failed » (échec)
CSCwk64418	Protocole NTP ne se synchronise pas lors de l'utilisation de l'authentification SHA-1
CSCwk64709	Échec de mise à mise à niveau de FXOS en raison d'un manque d'espace disponible dans /mnt/pss (isan.log consomme la majeure partie de l'espace)
CSCwk68759	Problème de déconnexion cérébrale dans le basculement HA en raison d'une panne sur le réseau du client
CSCwk71866	ASA : Le VPN de site à site entre les contextes sur le même périphérique perd le trafic en raison d'un « ipsec-tun-down »
CSCwk71992	Correctif de phase 1 de la vulnérabilité BlastRADIUS pour pix-asa – Authentificateur de message
CSCwk75030	Implémentation d'IPv6 dans le noyau Linux jusqu'à version 6.3 a un protocole net/ipv6/
CSCwk75033	Dans versions antérieures à version 1.21.3 de MIT Kerberos 5 (krb5), un agresseur peut provoquer une commande non va
CSCwk75035	Vulnérabilité dans le cœur du serveur HTTP Apache 2.4.59 et versions antérieures sont

ID du bogue	En-tête :
CSCwk75036	Déréférencement du pointeur nul dans mod_proxy du serveur HTTP Apache 2.4.59 et
CSCwk75956	ASA/FTD peut effectuer une recherche de la source et recharger dans le nom de fil SSH
CSCwk76142	Plantage de l'appareil de sécurité adaptable dans le fil PIX Garbage Collector avec inspect-rtsp activé
CSCwk77241	Panne du trafic en raison d'un épuisement du bloc 9k (tcpmod proc) observé sur FPR 3100 (HA)
CSCwk87457	ASA/FTD peut effectuer une recherche de la source et se recharger dans le nom de processus « lina » après le rechargement du périphérique
CSCwk88182	Recherche de la source FTDv50 en fonctionnement normal à PThread-8141
CSCwk89836	ASA/FTD peut effectuer une recherche de la source et recharger dans le nom de fil 'strlen'
CSCwk90679	Échec du test d'authentification Radius en raison d'une commande radclient manquante
CSCwk94382	FTD : Lina pourrait ne pas répondre à CONFIG_XML_REQUEST, ce qui entraînera le blocage des déploiements
CSCwk98990	Un grand nombre de fichiers de statistiques peut retarder les événements
CSCwm01544	Recherche de la source et rechargement de Lina dans le fil data-path
CSCwm02801	HA instable ce qui entraîne l'échec du déploiement
CSCwm04650	Augmenter l'utilisation de la mémoire, ce qui entraîne des retours en arrière dans Lina.
CSCwm05155	Snort AppID identifie incorrectement le trafic SSH comme inconnu
CSCwm05520	Désactiver le décodage des témoins syn de grappe lorsque la grappe FTD est déployée avec un ensemble en ligne
CSCwm07389	Erreurs de groupes C dans le journal système de l'appareil de sécurité adaptable lors de chaque redémarrage
CSCwm12434	La vérification de l'état de préparation doit être en place pour les fichiers de journalisation d'annulation/ibdata plus volumineux
CSCwm12751	Vulnérabilité suivante résolue dans le noyau Linux : a
CSCwm12757	Vulnérabilité suivante résolue dans le noyau Linux : t
CSCwm12909	Problème découvert dans la bibliothèque client C AMQP (alias Rabbitmq-c)
CSCwm13141	L'interface de ligne de commande/l'interface de ligne de commande FTD est verrouillée lorsque vous tentez d'exécuter une commande d'affichage

ID du bogue	En-tête :
CSCwm13199	Le trafic SIP est affecté en raison d'un comportement inattendu avec les non-traductions NAT.
CSCwm14509	Abandons incorrects vus avec une longueur non valide pour les types IE 23, 24 et 25 lors de l'inspection GTP
CSCwm14561	ASA/FTD peut effectuer une recherche de la source et un rechargement dans le nom de fil « fover_parse »
CSCwm14729	Matériel : l'appareil 3110 ne redémarre pas après une panne de courant, ce qui nécessite un cycle d'alimentation manuel
CSCwm29469	FMC GUI a une limitation à n'afficher que 50 règles SSH pour FTD (sous Paramètres de la plateforme – SSH)
CSCwm31193	Des événements ou des statistiques sont manquants après les journaux du gestionnaire d'événements « Erreur de chargement du module d'entrée »
CSCwm36646	Après la mise à niveau de FMC, FTDv en veille perd son niveau de performance pour FTD à haute disponibilité
CSCwm42745	Tunnels dynamiques de site à site bloqués dans l'état IN-NEG lorsque IKE_AUTH est manqué

Bogues résolus dans la version 7.2.8.1

Dernière mise à jour du tableau : 26/08/2024

Tableau 27 : Bogues résolus dans la version 7.2.8.1

ID du bogue	En-tête :
CSCwk62296	Vulnérabilité dans l'adresse SSP OpenSSH regreSSHion

Bogues résolus dans la version 7.2.8

Dernière mise à jour du tableau : 24-06-2024

Tableau 28 : Bogues résolus dans la version 7.2.8

ID du bogue	En-tête :
CSCwh83021	Paire de routes EIGRP ASA/FTD à haute disponibilité vidées après le basculement
CSCwj86116	UC LINA élevée observé en raison de la configuration NetFlow
CSCwj86341	L'assistant de mise à niveau de défense contre les menaces ne parvient pas à lancer l'installation des correctifs rapides sur les grappes FTD

Bogues résolus dans la version 7.2.7

Dernière mise à jour du tableau : 29-04-2024

Tableau 29 : Bogues résolus dans la version 7.2.7

ID du bogue	En-tête :
CSCwi63113	SNMP activé entraînant une boucle de démarrage de Cisco FTD après un rechargement ou une mise à niveau

Bogues résolus dans la version 7.2.6

Suite au bogue [CSCwi63113](#), la version 7.2.6 a été reportée le 29-04-2024 et n'est plus téléchargeable. Si vous l'avez téléchargée, ne l'utilisez pas. Si vous utilisez cette version, effectuez la mise à niveau. Les bogues répertoriés ici sont également corrigés dans la version 7.2.7.

Tableau mis à jour le : 22-04-2024

Tableau 30 : Bogues résolus supplémentaires dans la version 7.2.6-168 (Centre de gestion uniquement)

ID du bogue	En-tête :
CSCwj66339	OGO modifie l'ordre du contenu du groupe d'objets personnalisés, ce qui entraîne une panne au niveau de la NAT statique

Tableau mis à jour le : 25/02/2025

Tableau 31 : Bogues résolus dans la version 7.2.6-167 (toutes les plateformes)

ID du bogue	En-tête :
CSCvg00130	VPN d'accès à distance FTD : le changement de nom de l'ensemble d'adresses IP et du nom de profil de connexion entraîne l'échec du déploiement
CSCvj09334	ASA syslog 113005 n'affiche pas l'adresse IP de l'utilisateur
CSCvo58100	Valeur non valide fournie pour le paramètre d'entrée : « ? »
CSCvo67978	la commande « test aaa authentication » affiche une valeur de délai d'expiration incorrecte
CSCvr50778	FDM ne déploie pas « crypto IKEv1 am-disable » lorsque le mode dynamique doit être désactivé
CSCvt43334	Les cœurs générés en raison d'un arrêt attendu ou progressif doivent être nettoyés
CSCvu95526	L'option de désactivation « ca-check » devrait être disponible sur FDM.
CSCvw31514	L'appareil de sécurité adaptable ne parvient pas à établir la connectivité SSL avec les serveurs à l'aide du certificat auto-signés
CSCvx09047	L'activation de la fonction SSO avec une configuration aucune ou incorrecte redémarre constamment le processus auth-daemon

ID du bogue	En-tête :
CSCvx21458	FMC affiche une erreur lors de l'édition de la liste de préfixes associée à la carte de routage active dans le protocole BGP
CSCvx37329	Suppression des messages Syslog 852001 et 852002 dans la protection pare-feu contre les menaces
CSCvx44261	SNMPv3 : les caractères spéciaux utilisés dans la configuration SNMPv3 de FXOS provoquent des erreurs d'authentification
CSCvx52042	La mise à niveau vers la version 6.6.1 a échoué à 800_post/1025_vrf_policy_upgrade.pl
CSCvx52944	L'affichage de l'appareil de sécurité adaptable devrait inclure les messages récents de dpdk.log dans la mémoire flash
CSCvx69675	Défaillances majeures de FXOS concernant la panne de l'hôte de l'adaptateur et de l'interface virtuelle.
CSCvy11606	Erreur lors du chargement des données : Impossible de résoudre quelques-uns des BB de STDACE
CSCvy79686	FMC ne communique pas la fin de la session d'utilisateur administrateur pour les domaines dans un domaine FMC non descendant
CSCvz56980	Obtention d'objets de catégories d'URL non traitables lors de l'utilisation de l'appel d'API
CSCvz71215	FMC envoie des commandes de moniteur SLA dans un ordre incorrect, ce qui entraîne l'échec du déploiement.
CSCvz92730	Empêcher le processus snmpd d'être généré sous FTD pmtool
CSCwa22766	FMC4500/4600 affiche une licence virtuelle
CSCwa36703	Après la mise à niveau de FMC, la tâche de migration des données d'événements ne se termine jamais et n'affiche aucun progrès
CSCwa70323	Impossible de pousser des domaines supplémentaires > 1024 caractère, dans le cadre de l'attribut personnalisé sous Anyconnect VPN
CSCwa93215	Nœud principal déconnecté de la grappe VPN lors du basculement de la haute disponibilité sur le serveur principal avec recherche DNS
CSCwa95060	« SFDDataCorrelator:Parser [ERROR] Syntax error » sur le périphérique FTD
CSCwb06575	Le système d'exploitation Windows 11 n'est pas sélectionnable lors de la création d'un enregistrement DAP par l'intermédiaire de FMC
CSCwb41189	Correction de la synchronisation de l'horloge LINA
CSCwb55243	Il arrive que les informations de plantage du SNORT3 ne parviennent pas à collecter toutes les trames

ID du bogue	En-tête :
CSCwb61402	Les références LDAP/AD inaccessibles peuvent entraîner des retards ou des délais d'authentification extérieure sur FMC
CSCwb61408	FMC : N'a pas supprimé les utilisateurs d'authentification extérieure inutiles de /etc/passwd
CSCwb71519	Amélioration : F1661 - plus de détails sur le motif de l'échec et l'emplacement du journal
CSCwb75691	DBCheck.pl affiche les avertissements pour « health_alarm_static.healthmon_module_id »
CSCwb79062	L'interface graphique FMC n'affiche pas le nombre correct d'objets réseau inutilisés
CSCwb80789	Les connexions TLS 1.3 aux sites précédemment déchiffrés peuvent échouer
CSCwb85132	La page de mise à niveau des périphériques peut ne pas se charger lorsque la sélection du périphérique comporte des grappes FTD/des paires à haute disponibilité
CSCwb94431	Compteur d'échec du RPF MFIB au lieu d'autres abandons lorsque la liste des interfaces sortantes est nulle
CSCwb95850	Snort en panne en raison de fichiers lua manquants à cause de détecteurs d'applications désactivés (côté PM)
CSCwc13477	FMC : Échec de la mise à jour de l'interface Impossible de trouver l'interface source
CSCwc15032	Impossible de configurer la suppression/le seuil pour une règle de prévention des intrusions
CSCwc30573	Bouton de déploiement/tâches non visible dans FMC_UI lors des tests de mise à niveau configurés dans le thème clair
CSCwc31953	Prévention des fuites de clé privée RSA, quelle que soit la cause première.
CSCwc39525	Alerte d'état de la haute disponibilité du FMC « dégradé – maintenance » reçue périodiquement après la mise à niveau
CSCwc41805	La mise en correspondance des événements de corrélation sur le résultat en ligne de l'événement d'intrusion ne fonctionne pas correctement
CSCwc44419	ASA/FTD peut effectuer une recherche de la source et se recharger dans le nom du fil : fover_health_monitoring_thread
CSCwc49655	FTPS obtenant ssl3_get_record : type d'enregistrement incorrect lors de la connexion pour les règles KK et DR
CSCwc59564	Amélioration de la serviceabilité de la haute disponibilité : ajout du module de pulsation à haute disponibilité dans le plan de données
CSCwc60227	L'interface graphique FMC contourne le délai d'expiration de session tout en restant dans un onglet d'événement si l'intervalle d'actualisation est activé

ID du bogue	En-tête :
CSCwc74271	Le processus Auth-Daemon est redémarré continuellement lorsque l'authentification unique est désactivée dans la configuration de la haute disponibilité
CSCwc78689	Impossible d'enregistrer la configuration de domaine, sauf si le mot de passe AD Join est vide
CSCwc78697	L'appareil n'est pas marqué comme modifié lorsque Stocker moins d'événements sur FMC ou la journalisation du plan de données est activée dans SAL
CSCwc88118	La politique d'identité a pris du temps pour afficher le menu des ports disponibles
CSCwc93687	Message d'erreur lors de la modification de l'ACP
CSCwc94148	La page de déploiement ne se charge pas si l'état d'une grappe FTD ou d'un périphérique à haute disponibilité n'est pas approprié dans la base de données
CSCwc98050	La configuration de l'interface de gestion ASAv- du nœud du contrôleur n'est pas répliquée sur le nœud de données nouvellement rejoint
CSCwd03246	L'interface utilisateur ne respecte pas le délai d'expiration de la session en mode temps réel
CSCwd04436	Le téléchargement d'utilisateur/groupe peut échouer si un autre domaine est modifié et enregistré
CSCwd07098	SFP 25G CU ne fonctionne pas en netmod 8x25G dans Brentwood
CSCwd08098	cacert.pem sur FMC a expiré et tous les périphériques sont désactivés.
CSCwd10121	Requête non valide vue dans MonetDB merovingian.log
CSCwd10822	Déclencheur de basculement en raison de la défaillance du moteur d'inspection de l'autre unité à cause d'une défaillance du disque
CSCwd14432	« Inspection Interruption » (Interruption d'inspection) est vu comme OUI, mais SNORT3 n'a pas redémarré
CSCwd24106	Le moniteur de connexion ISE affiche un état d'alerte inexact
CSCwd29891	Aucun événement pour la température du châssis FPR1010 sur le moniteur d'intégrité
CSCwd30298	FTD : Connexion de canal de données FTPS affectée par l'identité du serveur TLS et la sonde de découverte envoyées par FTD
CSCwd31806	ASAv affiche continuellement l'impression d'informations de plantage en boucle
CSCwd32952	Renseignements sur les périphériques actifs et en veille non disponibles dans les journaux FMC pendant l'interruption de la haute disponibilité de FTD
CSCwd34079	FTD : Recherche de la source et rechargement dans le processus nommé lina
CSCwd34413	Défaillance SEC-WEB-CLICKJACK sur FMC : directive d'ancêtres de trame manquante

ID du bogue	En-tête :
CSCwd39506	La règle par défaut DND de la politique SSL échoue en cas d'erreur de suite de chiffrement non prise en charge et d'erreur SKE.
CSCwd41986	Les interfaces de traceurs de paquets ne s'affichent pas dans l'interface utilisateur après la mise à jour du nom de l'interface de la minuscule à la majuscule
CSCwd42072	Échec de l'installation de la SRU
CSCwd42347	FMC n'affiche aucune alerte/avertissement lors du déploiement de modifications de liste de préfixes avec la même seq #
CSCwd45451	FMC : Script pour modifier le nom d'hôte/l'adresse IP sur les FTD lorsque l'adresse IP ou le nom d'hôte du FMC est modifié
CSCwd46182	Les défaillances de synchronisation périodiques ne sont pas signalées aux utilisateurs
CSCwd46780	ASA/FTD : Recherche de la source et rechargement dans le nom du fil : appAgent_reply_processor_thread
CSCwd53635	AWS : Échec du déchiffrement SSL avec l'interface de tunnel Geneve
CSCwd55642	Événements d'intégrité du cœur de CPU périmés vus sur l'interface utilisateur de FMC après la mise à niveau vers la version 7.0.0 et les versions ultérieures
CSCwd56296	Recherche de la source et rechargement Lina dans le nom de fil « IP Init Thread »
CSCwd57927	Interface utilisateur de FMC peut devenir indisponible et afficher le message « Les processus système démarrent » après la mise à niveau
CSCwd62729	FDM QW/QP : tout le trafic URL bloqué dans le test BAT/BQT
CSCwd65598	cdFMC : Cœurs SFDataCorrelator et carte utilisateur-groupe non mises à jour sur le capteur
CSCwd65781	Échec de téléchargement de l'enregistrement avec des caractères spéciaux - Erreur expirée
CSCwd66815	Modifications de Lina pour l'assistance en ligne – Recherche de la source Snort3 dans daq-pdts lors de la gestion du trafic basé sur FQDN
CSCwd75782	Erreur de test d'authentification extérieure FMC "La méthode de chiffrement est configurée, mais vous n'avez pas téléversé de certificat."
CSCwd77581	Vulnérabilité de déni de service dans le traitement des messages Cisco ASA et FTD Message ICMPv6
CSCwd78940	Les pièges ne sont pas générés dans UUT pour la modification de configuration dans le multicontexte
CSCwd80284	L'importation ou l'exportation échoue avec une erreur de back-end
CSCwd81538	Échec du trafic FTD en raison de l'épuisement du bloc 9344 dans peer_proxy_tx_q

ID du bogue	En-tête :
CSCwd83141	Filtres CCL/CLU ne fonctionnent pas correctement
CSCwd83441	FMC devrait afficher l'état des interfaces physiques FTD regroupées dans le canal de port
CSCwd84046	L'inscription SCEP de Microsoft ne parvient pas à obtenir le certificat d'identité de l'ASA – Impossible de vérifier PKCS7
CSCwd85073	Cœur de flux Snort3 trouvé init_tcp_packet_analysis
CSCwd86226	FMC en veille affiche FMC-HA comme en bonne santé lorsque l'unité active Sybase est en panne
CSCwd86783	La désactivation des guides de navigation à partir de userappid.conf ne fonctionne pas
CSCwd87129	erreur voyante sur les politiques d'accès sur FMC – « Erreur lors de la validation de la politique »
CSCwd87438	Amélioration du mécanisme de journalisation pour les journaux système
CSCwd89811	Le trafic échoue dans la mise en grappe Azure ASAv après un délai d'expiration de secondes
CSCwd91013	FMC Échec de déploiement dans csm_snapshot_error
CSCwd93316	Aucun avertissement d'interruption d'inspection lors du déploiement après la mise à niveau de FMC
CSCwd93376	Les utilisateurs de VPN sans client ne peuvent pas télécharger de fichiers volumineux par le biais du portail WebVPN
CSCwd95043	Vulnérabilité de détournement de requêtes côté client pour les services client Cisco ASA et FTD VPN
CSCwd96845	Vulnérabilité de contournement de la liste de contrôle d'accès Cisco ASA et FTD AnyConnect
CSCwd97020	ASA/FTD : Échec de l'authentification SAML du fournisseur d'identité externe avec le message de demande incorrecte
CSCwd99592	Optimisation du chargement de la barre latérale pour la page HealthMon
CSCwe01977	ASA/FTD peut effectuer une recherche de la source et se recharger après un rechargement avec DHCPv6 configuré
CSCwe03631	Nécessité de fournir une limite de débit pour « l'historique de journalisation<mode> »
CSCwe04746	Alerte d'intégrité « No Traffic » imprévue sur l'interface de données à haute disponibilité de secours où aucune donnée ne circule
CSCwe06826	Alerte par courriel envoyée incorrectement pour une sauvegarde réussie de la base de données

ID du bogue	En-tête :
CSCwe10872	Erreur interne lors de la modification des configurations PPPoE
CSCwe11754	Les nœuds échouent de façon aléatoire à se joindre à la grappe en raison d'une erreur de mise en grappe interne
CSCwe12645	L'état secondaire bascule entre « Ready » et « Failed » lorsque le nœud est redémarré et que l'interface de gestion est fermée.
CSCwe13627	FMC Impossible de récupérer les journaux de dépannage du VPN.
CSCwe14062	Recherche de la source et rechargement FTD/Lina ou ASA liés au fil ctm_qat_engine
CSCwe14590	Aperçu du déploiement de FMC affichant une configuration complète au lieu de delta.
CSCwe16730	Échec de déploiement – « Erreur lors de l'impression du contenu du fichier de réponse show-xml-response » Réponse XML trop grande
CSCwe18446	Prise en charge de la grappe pending_rejoin dans la plateforme virtuelle FTDv
CSCwe18472	[FTD Multi-Instance] [SNMP] – Les OID de CPU renvoient une liste incomplète des CPU associées
CSCwe19051	L'alerte d'utilisation élevée du disque non géré FTD est déclenchée en raison des fichiers stockés dans l'emplacement /ngfw/Volume/root1/
CSCwe19830	Échec du déploiement de la politique « error executing /*!40101 SET character_set_client = @saved_cs_client */; * »
CSCwe20634	Vulnérabilité d'injection HTML du logiciel Cisco Firepower Management Center
CSCwe20641	Vulnérabilité d'injection HTML du logiciel Cisco Firepower Management Center
CSCwe21037	L'alerte d'utilisation de Snort mem doit être compatible avec la valeur de top.log
CSCwe21831	Ajouter un avertissement aux paramètres de la plateforme FTD lorsque le niveau de journalisation des paramètres de journalisation VPN est informatif
CSCwe22254	Après la désactivation de l'analyse des programmes malveillants, utilisation élevée du disque sur /dev/shm/snort
CSCwe22431	[SXP-UserIP Muted Leader] La jonction FMC à haute disponibilité purge le mappage IP_SGT de FW et rediffusions dans les capteurs enregistrés.
CSCwe25154	KP – cœur.SAMsgThread créé lors du basculement de la haute disponibilité dans le multicontexte
CSCwe25187	Authentification extérieure FMC obtenant une « erreur interne »
CSCwe26342	Recherche de la source ASA et rechargement citant le nom du fil : asacli/0
CSCwe26612	FTD prend plus de temps que prévu pour former des contiguïtés OSPF après un basculement de basculement
CSCwe27503	Classe de journalisation Prise en charge pour le routage

ID du bogue	En-tête :
CSCwe28362	Les règles de copier et coller sont interrompues et fournissent un message d'erreur vide dans la politique d'ID
CSCwe28874	Échec de l'enregistrement du FTD en raison de chaînes de canaux vides et du fichier HA_STATE manquant
CSCwe28912	FPR 4115 : l'unité principale a perdu toute la configuration à haute disponibilité après la mise à niveau de ftd à haute disponibilité
CSCwe29381	L'arbitre Sybase n'est pas opérationnel sur FMC à haute disponibilité
CSCwe29498	Échec occasionnel de chargement de light-modal-ac-rule-xx.css avec une erreur net::ERR_TOO_MANY_RETRIES
CSCwe30359	Le trafic chute avec une évaluation très élevée des règles sur SNORT
CSCwe30687	Fuite de mémoire dvti sur mp_counter_alloc
CSCwe33282	FTD : La mise à niveau a échoué, car le processus httpd n'était pas en cours d'exécution
CSCwe34269	L'erreur DBCheck n'est pas claire lorsque monetdb est à l'état « crashé »
CSCwe34664	L'interface est supprimée du groupe d'interfaces si l'utilisateur en modifie le nom [API]
CSCwe38353	Les PDU stream_tcp ne capturent pas l'ID de VLAN
CSCwe39514	Journaux de cache de l'hôte inondant la boîte
CSCwe41766	FTD peut ne pas redémarrer comme prévu après la mise à niveau si la version FXOS groupée est la même sur l'ancienne et la nouvelle version
CSCwe42582	Erreur lancée lors de la création/mise à jour de la règle CA et enregistrement après la création de l'index
CSCwe43965	Supprimer la limite de 30 caractères dans le nom de la règle lorsqu'une règle est déplacée de l'ACP vers le préfiltre
CSCwe44099	Appareil de sécurité adaptable Cisco et vulnérabilité DoS VPN SSL virtuel FTD
CSCwe45211	Nécessité d'alerter les utilisateurs avant de déclencher un déploiement complet sur FTD géré par FDM
CSCwe45879	Erreurs fréquentes observées concernant les échecs de chargement des fichiers en bloc qui n'existent pas
CSCwe47485	FTD : Lenteur de la CLISH en raison de l'invite LINA de verrouillage d'exécution de la commande
CSCwe48399	La fonction d'API publique BIO_new_NDEF est une fonction d'assistance utilisée pour str

ID du bogue	En-tête :
CSCwe48997	FDM : Impossible de créer plusieurs profils de VPN d'accès à distance avec différents serveurs SAML qui ont le même IDP\2028
CSCwe49185	La génération du mot de passe ne répond pas aux exigences en mode CC
CSCwe51296	Impossible de supprimer la politique de groupe de RAVPN via l'API REST
CSCwe51489	Impossible de traiter l'erreur de requête sur les événements; Interface utilisateur du FMC; Nombre maximal de connexions monetdb atteint
CSCwe52499	NGIPSv syslog-tls.conf.tt nécessite le retrait des filtres en mode CC
CSCwe53089	L'utilisateur appartenant à un sous-domaine ne peut pas collecter le traceur de paquets
CSCwe54999	Protocole en panne avec des instances de CPU inférieures sur ESXi 8 pour ASAv et FTDv
CSCwe55556	La journalisation est désactivée si les règles SSL sont réordonnées
CSCwe56452	Configuration IPv6 de BGP : association de carte de routage avec le voisin non déployée
CSCwe57218	FMC : état incorrect du rôle de grappe FTD ce qui entraîne une impossibilité de mise à niveau de FTD
CSCwe58207	Fuite de mémoire observée sur ASA/FTD lorsque l'historique de journalisation est activé
CSCwe58323	Erreur FMC EIGRP Pour la chaîne d'entrée : « route-map » lors de la configuration de l'EIGRP après la mise à niveau 7.2
CSCwe58620	Page des événements de connexion FMC « Erreur : impossible de traiter cette requête. Communiquez avec le service d'assistance. »
CSCwe58635	Échec de la vérification de la disponibilité [ERREUR] Erreur irrécupérable : la vérification de l'intégrité de l'objet entreprise a échoué avec des erreurs
CSCwe58980	/var/sf/QueryPoolData se remplit des répertoires d'entrepôt
CSCwe59664	La politique DAP créée dans l'interface graphique de FMC, pour détecter un système d'exploitation Windows avec un correctif rapide, ne fonctionnera pas comme prévu
CSCwe59889	La création d'un moteur de services d'identité par l'intermédiaire de l'API renvoie l'erreur du client 404 : Not Found
CSCwe61599	FTD 2100 - Mise à jour du mempool daq-ioq pour aider à la protection contre la corruption de la mémoire tampon
CSCwe61703	Impossible de supprimer l'attribut personnalisé AnyConnect --Dynamic-Split-Tunnel de la politique de groupe
CSCwe62951	Les db FSIC comprennent des fichiers de code d'octet Python et peuvent entraîner une alerte d'intégrité et un échec de l'intégrité du système.

ID du bogue	En-tête :
CSCwe63493	Après la restauration de la sauvegarde, plusieurs processus ne sont pas activés. Aucune erreur n'est observée lors de la sauvegarde ou de la restauration.
CSCwe63759	Correctifs de renforcement de grappe
CSCwe66137	L'utilisateur SSO se connecte à l'interface utilisateur de FMC si des informations d'authentification d'utilisateur local valides sont préremplies dans le navigateur
CSCwe66360	Snort3 manque de mémoire et le processus s'est arrêté de manière inattendue en raison d'une mémoire non libérée par les flux
CSCwe67180	Échec de synchronisation de l'application FTD à haute disponibilité en raison d'une corruption dans les fichiers de cache.
CSCwe69388	FMC poussant incorrectement l'attribut personnalisé AnyConnect « defer » comme « Defer » SENSIBLE À LA CASSE
CSCwe69824	Vérification de la validation sur l'interface graphique de FMC : ce qui provoque des problèmes et envoie des erreurs lors de l'ajout de nouveaux objets NAT
CSCwe71084	La clause IN ne fonctionne pas pour les requêtes d'externisation après la mise à niveau vers la version 7.0.x
CSCwe71238	Les demandes de la page de renseignements échouent après l'arrêt de RMQ pendant un certain temps
CSCwe72330	Recherche de la source FTD LINA et rechargement dans le fil Datapath après l'ajout du routage statique
CSCwe74899	L'erreur de synchronisation de l'application CD est « Échec de l'application de la configuration de l'application » sur le périphérique secondaire/en veille après la restauration de la sauvegarde sur le périphérique RMA
CSCwe75055	[Migration du modèle FMC] Surveillance de l'intégrité sur FMC signalant des erreurs
CSCwe75267	Impossible de forcer l'interruption de la paire FTD HA
CSCwe76036	Le message d'erreur ndclientd « Local Disk is full » doit fournir des détails de montage complets
CSCwe78377	Détection du réseau : problèmes de performance causés par l'utilisation de l'objet réseau \u2018any\u2019 dans les règles
CSCwe78674	Le téléchargement de groupe d'utilisateurs récupère moins de données qu'il n'y en a ou échoue avec l'erreur « Size limit exceeded »
CSCwe79954	La configuration d'authentification extérieure LDAP ne parvient pas à se déployer sur FTD si le même serveur LDAP est ajouté en tant que principal et de secours
CSCwe80273	La page de recherche des périphériques FMC supprime les FTD des groupes et les remet dans une unité non groupée

ID du bogue	En-tête :
CSCwe80915	Les informations sur les événements d'intrusion sous l'onglet des statistiques sont vides
CSCwe81135	La section de règle de la politique d'ac-policy affiche une page d'index inexistante dans l'ancienne interface utilisateur de la politique d'ac-policy
CSCwe81274	Tous les groupes d'objets réseau correspondants ne sont pas répertoriés si les objets réseau sont filtrés par nom
CSCwe81449	Déplacement de la journalisation de l'agent d'application vers un mécanisme de journalisation asynchrone (identique au protocole SNMP).
CSCwe81841	FXOS doit fournir une commande qui affichera le nombre d'heures de puissance totale du châssis/de la lame
CSCwe82631	FMC ne permet pas de créer plus de 30 interfaces VLAN
CSCwe82766	Le déploiement [Azure FMCv] avec l'option de clé SSH n'ajoute pas les clés correctement.
CSCwe85156	FTD : les interfaces complètes/10 Gbps ont été remplacées par 1 Gbit/s/auto après la mise à niveau et l'état d'arrêt
CSCwe85439	Modifier les codes de couleur pour représenter les processus à l'état « En attente »
CSCwe86029	Erreur d'authentification de la restauration du système FMC lors de la recréation d'image de FMC lors de l'utilisation du protocole FTP/SCP
CSCwe86350	L'alerte par courriel d'une activité planifiée ne fonctionne pas après la mise à niveau à la version 7.2
CSCwe86687	Le chargement de fichiers Apache Commons dans les versions antérieures à 1.5 ne limite pas le nombre de demandes
CSCwe86690	Dans Apache MINA, une demande HTTP malformée spécifiquement conçue peut entraîner
CSCwe86693	Un problème dans protobuf-java a permis l'entrelacement de com.google.protobuf
CSCwe86923	Dans Apache MINA, une demande HTTP malformée spécifiquement conçue peut entraîner
CSCwe86951	Certaines configurations mod_proxy sur les versions 2.4.0 du serveur HTTP Apache
CSCwe87134	ASA/FTD : Recherche de la source et rechargement en raison d'un débit élevé de trafic SCTP
CSCwe87789	Script pour déclencher la haute disponibilité lorsque le seuil de mémoire RSS dépasse le seuil configurable
CSCwe87831	La réponse de l'interface utilisateur du FMC est très lente : Ajouter l'accessibilité de la surveillance du module d'intégrité FMC ntpd

ID du bogue	En-tête :
CSCwe88496	« Échec de la conversion des règles personnalisées SNORT 2. Consultez /var/sf/htdocs/ips/snort.rej pour obtenir plus de détails. »
CSCwe88802	Préparation et mise à niveau de FTD réussies avec le journal d'exceptions comme « ProgressReport » n'a pas d'attribut « KB_UNIT »
CSCwe88808	Interface utilisateur du FMC bloquée après la vérification de la compatibilité
CSCwe89024	FTS sous la page de liste des politiques AC avec « obj » donne erreur « Erreur Moving Data » avec CTS DB
CSCwe89305	Échec de la migration de vFMC300 vers FMC2600 avec erreur « migration de R à N n'est pas autorisée »
CSCwe89818	L'authentification extérieure sur FMC peut lancer l'erreur « Can't use string ("") as a HASH ref while "strict refs" in use »
CSCwe90168	Impossible d'accéder à l'interface graphique de FMC lors de l'utilisation de l'authentification par certificat
CSCwe90195	Les règles locales ne s'affichent pas dans l'interface utilisateur après la conversion de Snort2 à Snort3 dans FMC 7.2.4-82
CSCwe90596	Détection de flux d'éléphants désactivée sur FMC, activation sur FTD après déploiement aléatoire
CSCwe91652	Échec de la sauvegarde de la base de données sur KVM FMC
CSCwe91738	Améliorer la convivialité pour gérer uniquement les flux TLS 1.3 lorsque le déchiffrement TLS 1.3 n'est pas activé
CSCwe91958	Les événements de corrélation basés sur les événements de connexion ne contiennent pas le contenu de la catégorie Security Intelligence
CSCwe92723	Retard de la phase 2 NAP observé dans la version 7.0.1 lors du déploiement de la politique
CSCwe93061	FTD ne renvoie aucune sortie de « show elephant-flow status » lorsque le contenu du fichier efd.lua est vide
CSCwe93137	KP - multimode : recherche de la source ASA observée lors de l'interruption et du regroupement du nœud à haute disponibilité.
CSCwe93162	FP1140 7.0.4 Le déploiement continue d'échouer avec l'erreur « Impossible d'utiliser une valeur non définie comme référence de hachage »
CSCwe93489	La détection des menaces ne reconnaît pas les objets d'exception avec un préfixe dans IPv6
CSCwe93558	Vulnérabilité d'injection de commande à distance SSH pour appareil de sécurité adaptatif Cisco

ID du bogue	En-tête :
CSCwe93566	Nécessité de désactiver la prise en charge par défaut de TLS 1.1 (déprécié) pour l'interface graphique de FDM
CSCwe93736	ASA ne met pas à jour le fuseau horaire malgré les commandes.
CSCwe94789	Le champ de négation DNS Umbrella du domaine de contournement n'est pas généré par FMC.
CSCwe95462	Cœurs de surveillance de l'intégrité en raison d'alertes d'intégrité avec plus de 8 champs
CSCwe95729	Vulnérabilité de contournement de l'authentification Cisco ASA et FTD SAML
CSCwe95797	Page SecureX dans l'interface graphique de FMC vide après la mise à niveau de FMC
CSCwe96062	Les paramètres de la plateforme ont permis à Syslog d'ajouter le protocole TCP avec le port 514
CSCwe97094	Traceur de paquets à lancement croisé à partir de la page des événements unifiés
CSCwe97939	Grappe ASA/FTD : modification du délai de réplication de la grappe avec augmentation de la valeur maximale de 15 à 50 secondes
CSCwe98319	Les redémarrages multiples d'ASAConfig présentent une fuite de mémoire de 16 K dans chaque redémarrage, ce qui entraîne une mémoire saturée de ZMQ.
CSCwe98430	Échec du déploiement de la politique AC sur les versions 7.2.4 FMC à 6.7 FTD
CSCwe98435	Déploiement sélectif avec l'interface de ligne de commande de la politique d'identité (captive-portal) et de la politique SSL (dp-tcp-proxy)
CSCwe99905	Erreur lors de l'enregistrement du modèle de rapport
CSCwf00483	Processus SFTop10Cacher orphelins trouvés
CSCwf00514	Les fichiers RRD ne peuvent pas être mis à jour si l'horodatage est en avance en raison d'un décalage de l'horloge du système
CSCwf00736	Échec de la sauvegarde CSM dans la sauvegarde FMC en raison d'une modification du fichier pendant que TAR le lisait
CSCwf00804	Enregistrement de lot corrompu à l'occasion du gestionnaire d'événements – Journaux SFDataCorrelator « Erreur de désérialisation »
CSCwf01318	Le processus sfhassd ne s'exécute pas après la restauration de la version 7.4.0-1755 à la version 7.3.0-69
CSCwf02005	La mise à jour des données du bac de sable de la tâche ActionQueue lance une erreur SQL après la mise à niveau de la version 7.2.4
CSCwf02453	Le seuil de rechargement ne doit pas être une option sous afficher la mémoire
CSCwf03345	Récupération après des défaillances de RMU en raison du mauvais état du lien de contrôle

ID du bogue	En-tête :
CSCwf03912	Nouvelle interface de ligne de commande pour l'intervalle de configuration <code>clu_update/keepalive</code>
CSCwf04915	FP1000 : Veuillez mettre à jour les fichiers <code>asa.log</code> de LINA pour éviter les messages récursifs<date> Noms de fichier soumis à la rotation <code>.1.gz</code>
CSCwf06255	7.2.4-129 – Grappe GCP – Échecs de contrôle de l'intégrité
CSCwf06261	La surveillance de l'intégrité exporte la valeur de mesure de mémoire d'échange du SNORT négative
CSCwf06318	La vérification de la disponibilité doit être autorisée à s'exécuter sans suspendre la haute disponibilité du FMC
CSCwf08320	SSE ne met pas à jour les informations pertinentes après la première découverte d'un actif.
CSCwf08387	Version LSP non mise à jour vers la plus récente dans l'invite LINA dans <code>SSP_CLUSTER</code> avec la version 7.2.4.
CSCwf08790	La restauration FMC de la sauvegarde à distance échoue en raison de l'absence d'espace sur le périphérique
CSCwf09024	Journal de suivi incorrect concernant la transition d'état
CSCwfl0295	Snort3 ne ferme pas la poignée de fichier <code>pcap</code> et le disque se remplit
CSCwfl0422	« Échec du téléchargement du flux de Security Intelligence » affiché même s'il a réussi
CSCwfl187	TPK 3110 – INCOMPATIBILITÉ de la version du micrologiciel après la mise à niveau à la version 7.2.4-144.
CSCwfl12521	Impossible de charger la page de la politique de prévention des intrusions sur l'interface graphique de FMC
CSCwfl13674	Les déploiements peuvent entraîner la suppression de certains mappages d'utilisateurs RAVPN.
CSCwfl14031	Snort en panne en raison de fichiers <code>lua</code> manquants en raison de détecteurs d'applications désactivés (côté VDB)
CSCwfl14257	Conteneur FTD restauré à partir d'une sauvegarde ne s'enregistre pas dans FMC en raison d'une erreur d'envoi par l'homologue d'un mauvais hachage
CSCwfl15532	Alerte d'intégrité d'échec de synchronisation de la haute disponibilité générée pour les deux unités FMC dans la paire à haute disponibilité – HA récupéré par la suite
CSCwfl15863	Valeurs « <code>vpn-idle-timeout</code> » très spécifiques entraînent des déconnexions et des reconnexion continues de session SSL
CSCwfl15978	La version 0.4.23 de <code>xml2js</code> permet à un agresseur externe de modifier ou d'ajouter un nouveau progiciel

ID du bogue	En-tête :
CSCwf16679	Amélioration de la convivialité de la haute disponibilité : maintenir les statistiques des clients NLP à haute disponibilité et les compteurs NLP CTL à haute disponibilité pour la synchronisation actuelle de l'application
CSCwf17389	L'ASA accepte les assertions SAML rejouées pour l'authentification du VPN d'accès à distance
CSCwf18144	Les correctifs rapides Firepower ne doivent pas être autorisés à s'installer lorsqu'ils ont déjà été installés précédemment
CSCwf19562	Modifications des journaux d'éclairage écrits dans /var/log/tid_process.log
CSCwf19621	Impossible de modifier le nom ou le mode d'inspection de la politique de prévention des intrusions
CSCwf19681	FMC secondaire devrait permettre de modifier les détails de l'adresse IP/du nom d'hôte de FTD sous l'onglet de l'appareil
CSCwf20215	L'utilisateur admin doit être exclu du filtre d'accès de l'interface de ligne de commande
CSCwf20958	Aucun logrotate et la taille maximale n'est configurée pour le fichier Health.log
CSCwf21204	DBCheck ne devrait pas s'exécuter sur MonetDB si l'utilisateur collecte seul une sauvegarde de configuration
CSCwf22241	Les zones de sécurité ne s'affichent pas dans l'interface utilisateur de la politique AC
CSCwf22568	Échec de la création de FTD à haute disponibilité, ce qui entraîne l'affichage des périphériques dans un état incohérent sur le FMC
CSCwf22637	Remplacements de groupes d'objets réseau non visibles ou ne peuvent pas être modifiés à partir de l'interface graphique de FMC
CSCwf22854	Impossible d'ajouter des fichiers dont le nom comporte « \u » pour effacer la liste à partir de la page de résumé des programmes malveillants
CSCwf23868	Mettre à jour l'état de la configuration si la synchronisation est ignorée
CSCwf23997	Échec de la vérification de la disponibilité de la mise à niveau dans l'interface graphique pour tous les capteurs en raison des caractères de nom pour l'affichage des capteurs.
CSCwf24818	Impossible de modifier le mot de passe de l'utilisateur administrateur après la migration de FMC s'il y avait un accès LOM
CSCwf25144	Page de gestion des sauvegardes FMC affichant la vérification de la sauvegarde pour les capteurs FTD.
CSCwf25402	FMC – L'épinglage de certificat SSL d'importation à partir d'un fichier CSV peut entraîner l'échec du déploiement de la politique sur FTD
CSCwf25563	La liste des appareils prend plus de temps à se charger lors de la création d'une nouvelle politique CA

ID du bogue	En-tête :
CSCwf25642	Problème d'utilisation du disque et de performance élevés en raison de la taille des journaux d'annulation MariaDB
CSCwf26264	La page de restauration des sauvegardes FMC prend environ 5 minutes à se charger lorsque le stockage distant est inaccessible
CSCwf26350	L'utilisateur n'est pas informé de l'IPS dépendant lorsque l'importation de la politique échoue.
CSCwf26989	Bande passante_analyzer.pl quitte les fichiers après l'exécution
CSCwf28063	La déconnexion SSE interrompt les recherches dans le nuage après la restauration.
CSCwf30542	Plantage Snort3 trouvé lors du nettoyage d'un objet CHP
CSCwf30824	Ajouter la réinitialisation de CIMC en tant que récupération automatique pour les problèmes de blocage d'IPMI de CIMC
CSCwf32890	Connexion FMC SSH en veille souvent déconnectée
CSCwf33904	[IMS_7_4_0] – Échec de la mise à niveau de FDM virtuel : HA configStatus='OUT_OF_SYNC après UpgradeOnStandby
CSCwf34070	Vulnérabilité de déni de service ciblé pour l'authentification du VPN SSL de l'Appareil de sécurité adaptable et de FTD
CSCwf34123	La réorganisation des colonnes dans le concepteur de rapports présente des problèmes lors de l'utilisation d'Atomic
CSCwf34892	Inondation du fichier de trace de connexion, fo_chk_peer_down_ifcs
CSCwf35173	SFTunnel ne parvient pas à s'établir correctement en raison d'une erreur de configuration du fichier running_config.conf
CSCwf35223	SGT Dépannage de la capacité d'établir une corrélation avec l'adresse IP
CSCwf35233	DoS du logiciel de l'Appareil de sécurité adaptable et de FTD
CSCwf35346	FMC devrait gérer les erreurs de manière appropriée lorsqu'ISE signale une erreur pendant le téléchargement de SXP
CSCwf35500	FXOS/SSP : Système devrait offrir une meilleure visibilité des événements erreur corrigibles de DIMM
CSCwf36011	La règle d'abandon n'est pas supprimée lorsque l'unification snmp sur la lame est supprimée.
CSCwf36391	Le troisième paquet de pulsation n'est pas envoyé avant de déclarer la défaillance d'intégrité de l'application
CSCwf36419	ASA/FTD : Recherche de la source et rechargement avec le nom de fil « PTHREAD »
CSCwf36621	access-list : Impossible de combiner différents types de listes d'accès.

ID du bogue	En-tête :
CSCwf38782	Modification du message de journal système ASA-3-202010
CSCwf39163	ASAv : une latence élevée est expérimentée dans l'environnement Azure pour les paquets ping ICMP lors de l'exécution de snmpwalk
CSCwf39821	FTD : Unité de haute disponibilité heurtée à une erreur de synchronisation d'application de CD en raison d'une erreur de redémarrage de ngfwManager sur l'homologue
CSCwf40594	Wyoming/SFCN ASA : Valeurs incorrectes affichées dans l'interface de ligne de commande des objets crypto ssl
CSCwf40674	API REST [PUT] : PC appelé sans configuration h/w, la configuration h/w existante est définie à null dans la base de données
CSCwf41187	Les détecteurs WINSNP et SFTP ne fonctionnent pas comme prévu
CSCwf41433	IP du client ASA/FTD manquant dans la demande TACACS+ dans l'authentification SSH
CSCwf42012	Équilibrage de charge incorrect pour le trafic sur les interfaces ERSPAN sur FPR 3100/4200
CSCwf42234	Les détails du tunnel SVTI du tableau de bord S2S sont manquants après la mise à niveau
CSCwf43033	la couverture du silo diskmanager /var/sf/htdocs/img/dashboard/no-cache/ nécessite hwm et lwm beaucoup plus bas
CSCwf43247	Les tâches d'analyse de correction NMAP restent à l'état en attente dans la table d'attente des actions, ne sont pas effacées
CSCwf43850	ECMP + NAT pour la demande d'assistance des sessions ipsec pour Firepower.
CSCwf44621	Recherche de la source et rechargement sur le fil DataPATH-6-21369 et lié à la génération de l'ID de message syslog 202010
CSCwf44915	Les anciens paquets LSP ne sont pas élagués, ce qui entraîne une utilisation élevée du disque
CSCwf45091	Snort3 correspond à SMTP_RESPONSE_OVERFLOW (règle IPS 124:3) lorsque les hôtes SMTPS échangent des certificats
CSCwf45094	Le processus MariaDB dans FMC devrait utiliser jemalloc au lieu de glibc
CSCwf45106	Les instructions d'intégration de Securex SSE doivent être mises à jour
CSCwf49254	Impossible d'annuler l'enregistrement de FTD de Cisco Cloud dans FDM s'il est déjà désinscrit du côté du nuage
CSCwf49640	Afficher le dns ip-cache a d'anciennes offres après le changement de version de Snort, ce qui affecte la sortie de la surveillance de chemin d'accès.

ID du bogue	En-tête :
CSCwf52810	L'interrogation SNMP ASA ne fonctionne pas et affiche « Impossible de répondre à cette demande maintenant » sur les commandes d'affichage
CSCwf52821	Sauvegarde universelle : créer une sauvegarde unique pour FMC à haute disponibilité
CSCwf53210	[Amélioration] Le nombre d'archives de configuration doit être configurable à partir de l'interface utilisateur
CSCwf55014	Amélioration de la convivialité pour CSCwe28912 : état de la haute disponibilité en état d'échec.
CSCwf55236	Impossible de supprimer le groupe de règles personnalisées même lorsqu'il est exclu de toutes les politiques IP
CSCwf56291	La rétention des fichiers de configuration FMC revient aux valeurs par défaut si l'outil ca_purge a été utilisé avant la mise à niveau de la version 7.2.4
CSCwf56404	L'outil ca_purge doit redémarrer Tomcat
CSCwf57282	Mettre à jour le modèle EtherPIO pour prendre en charge le nouveau champ linkTs
CSCwf57315	Rapprocher l'état de FMC : La mise à niveau de FMC doit créer un fichier d'état de mise à niveau pour prendre en charge les protections de mise à niveau de FTD.
CSCwf57850	Le processus TelemetryApp continue de se quitter chaque minute après la mise à niveau du FMC
CSCwf57856	Recherche de la source FXOS et rechargement causés par une fuite dans la file d'attente de la mémoire tampon MTS
CSCwf59176	FXOS déclenche une défaillance pour l'interface de gestion désactivée par l'administrateur
CSCwf59571	FTD/Lina – Problème ZMQ HORS MÉMOIRE en raison d'une mémoire pool Msglyr inférieure sur certaines plateformes
CSCwf59643	FTD : Échec de synchronisation de l'application HA en raison d'un basculement de l'interface vers l'unité de secours
CSCwf61443	Vulnérabilité de script intersite du logiciel Cisco Firepower Management Center
CSCwf62103	FMC doit valider correctement les règles de politique QoS avant d'autoriser le déploiement sur FTD
CSCwf62729	Vulnérabilité du déni de service SSL/TLS de Cisco ASA/FTD Firepower 2100
CSCwf63256	Firepower se recharge de manière inattendue avec recherche de la source
CSCwf63358	FTD diskmanager.log est corrompu, ce qui fait que le module HM_du envoie une alerte de faux usage élevé du disque
CSCwf63589	Recherche de la source et redémarrage pour le processus snmpd sur Cisco FTD

ID du bogue	En-tête :
CSCwf63872	FTD prend plus de temps que prévu pour former des contiguïtés OSPF après un basculement de basculement
CSCwf64590	Les unités sont expulsées de la grappe de manière aléatoire en raison d'un HB manqué ASA 9.16.3.220
CSCwf66271	Impossible de répertorier l'interface dans la politique d'exclusion de périphérique
CSCwf66307	La politique d'exclusion pour exclure l'état de l'interface sera supprimée sur FMC après un certain temps
CSCwf66333	La sélection de « Toutes les interfaces » sous la politique d'exclusion de FTD pour le module d'état de l'interface ne fonctionne pas
CSCwf66387	Échec de la restauration de FTD [IMS_7_4_0] « La validation de l'état de gestion ne peut pas être effectuée, impossible de revenir en arrière »
CSCwf67337	FMC prend beaucoup de temps pour enregistrer les objets de remplacement, même s'ils ne sont pas modifiés
CSCwf68335	vFMC : échec du déploiement planifié
CSCwf69313	Événements de corrélation pour les règles du traceur de connexion <, <=, = ou != affichent les données pour les connexions non liées
CSCwf69475	L'option de transfert de paquets passe à NO automatiquement lorsque vous modifiez le nom du périphérique dans la gestion des périphériques
CSCwf69576	Plantage Snort avec le trafic d'inspection SMB
CSCwf71602	FMC ne génère pas d'alertes VPN FTD S2S en cas de panne ou d'inactivité
CSCwf73773	Échec du vidage des 20 derniers paquets de réponse à la demande rmu
CSCwf74319	Alerte d'intégrité pour une différence significative du nombre d'enregistrements reçus avec le téléchargement en bloc
CSCwf75214	L'ASA supprime le PSK distant IKEv2 si la chaîne de clé se termine par une barre oblique « \ » après le rechargement
CSCwf75695	Une grappe FTD en double a été créée lorsque plusieurs événements de grappe se produisent en même temps
CSCwf76369	mstolfp dans libntp/mstolfp.c dans NTP 4.2.8p15 a une écriture hors limite
CSCwf77995	Azure FTDv, géré localement par FDM, passe en boucle de cycle de démarrage/rechargement après le premier déploiement
CSCwf79279	recherche de la source pour le nœud vftd Azure lors du chargement de plusieurs objets de service réseau pendant ns_reload.
CSCwf79372	après l'interruption de la haute disponibilité, la liste sélectionnée affiche les deux appareils lorsqu'un appareil est sélectionné pour la mise à niveau

ID du bogue	En-tête :
CSCwf80163	L'agent Smart d'alerte critique n'est pas enregistré auprès du Smart Licensing Cloud
CSCwf81320	Impossible de configurer et de déployer le serveur DNS IPv6 pour RAVPN dans FMC 7.2.4
CSCwf82093	Lorsque les communications sont désactivées pour FTD à partir de l'interface utilisateur de FMC, le back-end affiche que la connexion reste activée.
CSCwf82279	Journalisation excessive des messages ssp-multi-instance-mode dans /opt/cisco/platform/logs/messages
CSCwf82447	La modification de la règle NAT d'identité désactive « effectuer une recherche de routage » en silence
CSCwf82644	Les flux du système autonome sont téléchargés bien que les mises à jour des flux soient désactivées par l'utilisateur
CSCwf84588	Désactiver définitivement TLS 1.1 pour la communication avec sftunnel
CSCwf86519	FMC affiche l'état du RPV comme inconnu, même si l'état est activé si l'un des homologues est extranet
CSCwf86557	Le déchiffrement des connexions du moteur/SSL se bloque avec l'erreur de l'interface PKI vue
CSCwf86860	Interface graphique FMC La page ACP devient vide et se bloque lors de la recherche dans les règles et du passage aux dernières pages
CSCwf87070	WM RM – L'état du port SFP 9 suit l'état du port SFP 10 11 12
CSCwf87348	Lorsque la liaison d'état est retournée, l'état de la haute disponibilité est passé de « de secours » à « synchronisation en bloc » sans raison de basculement
CSCwf88124	FPR 1010 –Les ports de commutation en mode de solutions de liaisons peuvent ne pas transmettre le trafic vlan après une perte de courant ou un redémarrage
CSCwf89959	ASA : ISA3000 ne répond pas aux interrogations SNMP d'OID entPhySensorValue
CSCwf91282	L'importation de .SFO dans FMC a échoué en raison de l'inclusion de règles locales ou de règles personnalisées ayant un champ de message de règle vide
CSCwf91381	Adi : journaliser le nom de domaine complet de l'hôte spécifique utilisé pour le téléchargement en bloc et les connexions de connecteur Web
CSCwf92047	Amélioration : FMC, désactivation de la création d'un client sous l'onglet eStremer dans l'interface graphique lorsqu'il fonctionne en mode UCAPL
CSCwf92182	Vulnérabilité d'injection SQL du logiciel Cisco Firepower Management Center
CSCwf92439	Déploiement bloqué en raison d'un objet de port avec une plage d'adresses IP maximale de 131 838 dans NAT64

ID du bogue	En-tête :
CSCwf92661	ASA FTD : Recherche de la source et rechargement en raison d'une corruption de tampon libre
CSCwf93293	Vulnérabilité de contournement du filtre de débit Snort de plusieurs produits Cisco
CSCwf94450	Nom du fil : DATAPATH en raison d'une corruption de la mémoire
CSCwf94677	La configuration « failover standby config-lock » est perdue après le rechargement simultané des deux unités à haute disponibilité
CSCwf95888	FPR1K Switchport transmet le trafic CDP
CSCwf98546	Les mini-vidages de Snort ne sont plus gérés par diskmanager après le passage à var/common
CSCwf99303	Interface utilisateur de gestion qui présente un certificat autosigné plutôt qu'un certificat personnalisé signé par l'Autorité de certification (CA) après la mise à niveau.
CSCwh00123	Dans le scénario multigestionnaire, cdFMC et FMC d'analyses, FTD ne doit recevoir que des flux d'identité de Config FMC
CSCwh00692	Recherche de la source @<capture_file_show+605 at ../infrastructure/capture/capture_file_finesse.c:282>
CSCwh02561	Changements de vitesse de l'interface de canal de port de 10 G à 1 G après le déploiement d'une politique
CSCwh04185	Plantage de Snort dans la réponse active
CSCwh04730	Plantage des segments de vérification des appareils de sécurité adaptables Cisco/FTD HA lorsque les tampons de mémoire sont corrompus
CSCwh05863	L'appareil de sécurité portable omet le port dans le champ d'hôte de l'en-tête HTTP de la demande OCSP si le port autre que le port par défaut commence par 80
CSCwh06452	Incompatibilité de vitesse d'interface dans la réponse SNMP utilisant l'OID .1.3.6.1.2.1.2.2
CSCwh08215	La mise à niveau de la version 7.2.x à la version 7.2.5 peut échouer si une valeur nulle est observée dans la vitesse/le duplex dans l'interface.
CSCwh08388	Interface GUI FMC n'enregistre pas les paramètres d'interface
CSCwh08403	FMC HA – Politique d'intégrité – Le nombre appliqué affiche « 0 » appliance
CSCwh08481	Recherche de la source ASA sur le processus Lina avec fonctions FreeB et VPN
CSCwh08683	FTDv/AWS – Décalage de l'horloge NTP entre Lina et la grappe FTD
CSCwh09113	FPR1010 en haute disponibilité n'a pas pu envoyer de données à GARP/ARP ou en recevoir, erreur « \edsa_rcv: out_drop\ »
CSCwh10087	défaillance du processeur en raison d'un nom de fichier principal avec un espace blanc

ID du bogue	En-tête :
CSCwh12009	Erreur d'échec EOStore s'affiche après la suppression de la couche de règle partagée.
CSCwh13474	Micrologiciel PSAQ (Power-Sequencer) – Retirer la vérification de l'ID de l'appareil
CSCwh13551	Onglet de tableau de bord du moteur de visibilité chiffrée (EVE) et gadgets non ajoutés à l'interface graphique de FMC lors de la mise à niveau
CSCwh13625	Onglet de tableau de bord FMC du moteur de visibilité chiffrée (EVE) et gadgets non renommés après la mise à niveau de la version 7.1 à la version 7.2 ou version ultérieure
CSCwh13821	ASA/FTD peut effectuer une recherche de source et rechargement lors de la modification de la taille du tampon de capture
CSCwh13916	Le déploiement de la politique AC échoue lors de la collecte des objets SNORT3
CSCwh14067	Vulnérabilité de déni de service Snort 2/3 pour trafic TCP/IP Cisco FTD
CSCwh14352	Mise à niveau de CiscoSSL Lina vers la version 1.1.1v et FOM 7.3a
CSCwh14731	L'authentification extérieure échoue si le nom de l'objet contient des espaces
CSCwh14863	La grappe FTD 7.0.4 abandonne les paquets SQLNet d'Oracle en raison d'un message tcp-not-syn
CSCwh16301	Statistiques de nombre de résultats incorrects sur la grappe ASA uniquement pour la sortie à l'échelle de la grappe
CSCwh16759	Le protocole SNMP ne fonctionne pas sur l'unité ASA active principale dans un environnement multi-contexte
CSCwh17052	Absence de validation de la longueur de chaîne lors de la création des noms d'objets ou de catégories à l'aide de l'API
CSCwh17576	L'état du tunnel VPN de site à site sur FMC ne fonctionne pas, même s'il est activé du côté de FTD
CSCwh18704	Certifi est une collection curée de certificats racine pour la validation de
CSCwh18967	Inclusion de « show env tech » dans le dépannage de FXOS FPRM
CSCwh19897	Grappe ASA/FTD : réutilisation du numéro de séquence TCP aléatoire sur deux connexions différentes avec le même 5 tuple
CSCwh21337	FTD – Problème avec le code de paquet LSP lors de la restauration du déploiement.
CSCwh21474	Recherche de la source ASA lors de la reconfiguration de la liste d'accès
CSCwh21772	Mise à niveau de FxOS CiscoSSL vers la version 1.1.1v et FOM 7.3a
CSCwh22317	Validation LILO manquante lors de la vérification de la disponibilité
CSCwh22348	Plantage de sfdatacorrelator en raison d'une corruption de la table « rua_event_XXXXX »

ID du bogue	En-tête :
CSCwh22783	La présence d'un gestionnaire périmés sur FTD après un échec d'enregistrement dans le cdFMC entraîne l'échec du nouvel enregistrement.
CSCwh22888	FXOS : Suppression de l'application de l'état dégradé des lames après plusieurs erreurs corrigibles de DIMM
CSCwh24321	FXOS : Alpertion 100G NetMod n'est pas reconnu correctement
CSCwh24826	Mise à niveau de FMC bloquée à 1039_fmc_rabbitmq_enable
CSCwh24901	« Déversement fréquent des événements (et non des événements non traités) à supprimer du FMC »
CSCwh25928	Les autorisations manquantes dans le rôle d'utilisateur FMC peuvent entraîner le redémarrage continu de Tomcat après la mise à niveau à la version 7.2.4
CSCwh27414	L'état de déploiement passera à l'état déployé juste après le début du déploiement, puis à l'état de déploiement
CSCwh27510	Négociation vers le secours froid prenant 30 minutes sur TPK avec 900 sous-interfaces
CSCwh28007	Lors de la modification des règles de politique AC, le numéro d'ordre des règles est mal aligné.
CSCwh28185	Les tâches dl_task.pl continuent d'être créées toutes les heures lorsqu'une requête de base de données est bloquée
CSCwh28206	Blocage de pare-feu des paquets après le basculement en raison de mappages SGT IP <->
CSCwh28779	Impossible d'enregistrer la politique de prévention des intrusions après la mise à niveau vers la version 7.x, car le nom dépasse 40 caractères
CSCwh30276	Le filtre de mise à jour de règle dans la politique de prévention des intrusions affiche des résultats incohérents
CSCwh30346	ASA/FTD : délai de basculement de 1 seconde pour chaque règle NAT de NLP
CSCwh30676	Échec de la connexion au système IP configuré sur l'interface de gestion
CSCwh31495	FTD – Recherche de la source et rechargement en raison d'une règle de NAT supprimée par le cœur de l'UC
CSCwh31502	Amélioration de l'opération de copie de Lina pour startup-config vers backup-config.cfg en haute disponibilité
CSCwh35088	Nombre de fichiers lina-io démarrés limité à 8 en raison de l'absence des fichiers journal fover sur la paire en haute disponibilité
CSCwh37475	Suppression des commandes msie-proxy lors de la restauration de flexconfig
CSCwh37737	La migration de flexconfig EIGRP FMC7.2.x échoue avec une erreur interne en raison d'une incompatibilité de configuration de l'interface

ID du bogue	En-tête :
CSCwh38492	La restauration FMC est bloquée à l'étape d'effacement du Vault après la restauration de MySQL
CSCwh39258	Il arrive que l'authentification extérieure ne fonctionne pas après le basculement de la haute disponibilité vers le mode actif
CSCwh40106	FTD hébergé sur KP abandonne incorrectement les paquets ESP décodés si l'action du préfiltre est analysée
CSCwh41094	Vulnérabilité de déni de service Snort 2/3 pour trafic TCP/IP Cisco FTD
CSCwh41305	Abandons occupés par Snort pour le trafic HTTPS via VPN avec moins de trafic - appauvrissement de 2K
CSCwh41922	Vulnérabilité d'injection HTML du logiciel Cisco Firepower Management Center
CSCwh41958	Vulnérabilité d'injection HTML du logiciel Cisco Firepower Management Center
CSCwh42077	Cisco_Firepower_GEODB_FMC_Update* ne sont pas inclus dans diskmanager
CSCwh42233	Certains ID de journal système ne peuvent pas être configurés dans les paramètres de la plateforme.
CSCwh42412	Bloc 9344 du FTD en raison d'un trafic GRE fragmenté sur le traitement du flux interne de l'interface d'ensemble en ligne
CSCwh43945	Une recherche de la source et un rechargement pour FTD/ASA peuvent se produire lorsque les débogages de paquets ssl sont activés
CSCwh44215	Amélioration – Exempte la sonde TSID de passer par l'inspection EVE
CSCwh44479	Échec de la création de l'archive de configuration et erreur de l'aperçu du déploiement
CSCwh47053	ASA/FTD peut rechercher la source et recharger dans le nom de fil « dns_cache_timer »
CSCwh47395	L'objet de liste d'accès étendu ne permet pas la configuration de la plage d'adresses IP.
CSCwh47701	L'appareil de sécurité adaptable permet le même processus de routage dynamique de BGP pour les données physiques et les interfaces de gestion uniquement
CSCwh48813	Dépassement de la mémoire tampon basée sur le tas dans la fonction bfd_getl32 dans Binutils objdump
CSCwh48844	FTD : Basculement/Haute disponibilité désactivé avec la version 0.0 n'est pas compatible
CSCwh49244	La commande « show aaa-server » affiche toujours la durée de la boucle moyenne 0 ms.
CSCwh50060	Certaines sondes TLS1.3 échouent en raison de rst+ack non envoyé par FTD pendant le délai d'expiration

ID du bogue	En-tête :
CSCwh52526	Délai d'expiration de l'authentification FMC lorsque la session utilisateur est active pendant plus de 1 h (délai d'inactivité)
CSCwh53116	Le pays et le continent de l'initiateur sont manquants dans l'affichage personnalisé sur la visionneuse d'événements
CSCwh53143	ASA : L'accès à la gestion par le tunnel IPSec ne fonctionne PAS
CSCwh53745	ASA : journaux inattendus pour lancer la connexion entrante pour la réponse à la requête DNS
CSCwh54477	Le FMC affiche l'alerte « La clé de chiffrement du mot de passe n'a pas été définie » pour un périphérique 11xx/21xx/31xx
CSCwh55178	Gérer la fuite de mémoire dans la commande de test Callhome
CSCwh55543	FMC 4600 v7.2.4 Gadget de tableau de bord EVE affichant des données corrompues
CSCwh56218	ASA : Recherche de la source et rechargement pendant la synchronisation de la grappe de 6 nœuds après la défaillance ou la récupération de la liaison CCL
CSCwh57976	Amélioration de l'utilisation de l'UC dans l'inspection SSL pour la gestion de l'algorithme de signature pris en charge
CSCwh58467	ASA n'envoie pas le piège SNMP 'warmstart'
CSCwh58490	Le déploiement de FMC a échoué en raison d'erreurs internes après la mise à niveau
CSCwh59199	Recherche de la source ASA/FTD et rechargement avec le VPN IPSec, ce qui pourrait entraîner une mise à niveau
CSCwh59222	SNORT3 - FTD – TSID cpu élevé, sondage DAQ lorsque SSL activé ne tire pas assez de paquets
CSCwh59557	Règle NAT source effectuant une traduction incorrecte en raison d'une surcharge de l'interface
CSCwh60504	LINA générerait aléatoirement un recherche de la source et un rechargement sur FPR-1K
CSCwh60604	ASA/FTD peut rechercher la source et se recharger dans le nom de fil « lina » lors du traitement des données DAP
CSCwh60631	Échec de réassemblage du paquet UDP fragmenté via le tunnel MPLS
CSCwh60778	Recherche de la source FTD et rechargement dans le traceur TLS pour le déchiffrement SSL TLS 1.3
CSCwh60783	FTD – Le portail captif activé est toujours en cours d'exécution, bien que la fonctionnalité soit désactivée
CSCwh62731	Mise à niveau de FTD de la version 6.6.5 à la version 7.2.5, suppression de l'OGS, ce qui entraîne une expansion des règles au démarrage

ID du bogue	En-tête :
CSCwh63588	La configuration de l'hôte SNMPv3 de FTD est supprimée d'IPTABLES après l'ajout de la configuration de groupe d'hôtes
CSCwh64704	FDM devrait fournir un moyen de désactiver le portail WebVPN sur FTD
CSCwh65128	LINA affiche que l'assistance technique ne parvient pas à être générée dans le cadre de sf_troubleshoot.pl (fichier de dépannage)
CSCwh66359	ASDM ne peut pas voir l'horodatage du journal après avoir activé l'horodatage de journalisation sur l'interface de ligne de commande
CSCwh66636	La configuration et la non-configuration du « match ip address test » peuvent entraîner la recherche de la source
CSCwh68482	Logiciel Cisco Firepower Threat Defense pour la série Firepower 2100
CSCwh68878	Le processus Diskmanager s'est terminé de manière inattendue
CSCwh69346	ASA : Recherche de la source et rechargement lors de la restauration de la configuration à l'aide de l'interface de ligne de commande
CSCwh69777	FTD – Affichage incorrect de l'utilisation de la mémoire SNORT élevée avec l'identité du serveur TLS
CSCwh69787	Vulnérabilité de script intersite du logiciel Cisco Firepower Management Center
CSCwh70323	Entrée d'horodatage manquante pour certains messages syslog envoyés au serveur syslog
CSCwh70481	La chaîne de communauté envoyée par le routeur ne correspond pas à l'ASA
CSCwh70842	Vulnérabilité d'injection SQL dans Cisco Firepower Management Center
CSCwh70866	Vulnérabilité de script intersite du logiciel Cisco Firepower Management Center
CSCwh70905	Communication de basculement perdue secondaire sur Intérieur, en utilisant IPv6, mais le prochain test d'Intérieur passe
CSCwh71161	ASA FTD : Recherche de la source et rechargement dans le fil Nom : Update_mem_reference
CSCwh71589	Coverity 886745 : OVERRUN in verify_generic_signature
CSCwh71665	Recherche de la source ASA sous match_partial_keyword lors du profilage de CPU
CSCwh72522	Erreur lors de l'enregistrement de RAVPN avec carte d'attributs LDAP contenant une entrée sans nom de mappage d'attribut Cisco
CSCwh73727	Snort3 abandonne le protocole IP 51
CSCwh74219	Échec de la mise à niveau de FMC 7.2.4.1 à 7.2.5 au niveau de 600_schema/000_install_fmc.sh

ID du bogue	En-tête :
CSCwh74586	XTLS : Avec le module d'extension configuré TSID AC-Policy ne se désengage pas immédiatement au niveau du châssis
CSCwh74870	Valeurs élevées inattendues pour le compteur en cours de la DAQ
CSCwh76959	FMC n'enregistre pas les modifications apportées à la liste d'accès.
CSCwh77348	ASA : Recherche de la source et rechargement lors de l'exécution de la commande « show nat pool détail » sur une configuration de grappe
CSCwh79095	Snort générant un nombre excessif de fichiers journaux unifiés par Snort avec zéro octet
CSCwh80131	S3_Core : crashinfo : augmenter l'espace tampon pour imprimer des noms de fonction plus longs
CSCwh83254	ASA/FTD : Recherche de la source et rechargement sur le nom de fil CP Crypto Result Processing
CSCwh84376	Dans FPR4200/FPR3100-HA/cluster, crashinfo/corefile.lina observé lors du redémarrage du périphérique.
CSCwh89289	Snort est rechargé pendant le déploiement en raison d'une plage temporelle et d'un contenu de conf NAP dans chaque exécution
CSCwh89835	Mots de passe FMC en texte brut pour le Serveur RADIUS et la phrase d'accès du certificat
CSCwh90018	des ID d'objets d'interface inutilisés peuvent être présents dans la configuration de zone après le réenregistrement de FTD
CSCwh90693	FTD annule l'enregistrement du FMC en veille immédiatement après un enregistrement réussi
CSCwh90813	Échec de la mise à niveau de FDM en raison de certificats expirés.
CSCwh91574	FTD : recherche de la source dans le nom de fil client_xml_request_process
CSCwh93649	La copie de fichier par le protocole SCP à l'aide de la pile ciscossh échoue avec l'erreur « no such file or directory »
CSCwh93710	La dernière règle trouvée affiche une valeur hexadécimale avant l'heure actuelle dans les appareils de sécurité adaptables Cisco (ASA) et ASDM
CSCwh95010	Recherche de la source imprévue sur le nom de fil Lina et le périphérique a connu un redémarrage
CSCwh95175	ASA/FTD peut rechercher la source et recharger dans le nom de fil « lina »
CSCwh99331	journal système non généré « ASA-3-202010 : Pool NAT épuisé » lors du passage du trafic d'iLinux à oLinux
CSCwi01085	Recherche de la source FTD VMWare à l'adresse PTHREAD-3587

ID du bogue	En-tête :
CSCwi01381	ASA/FTD peut rechercher la source et recharger dans le nom de fil « lina »
CSCwi01895	Connexion interrompue pendant les transferts de fichiers en raison d'une défaillance de HeartBeat
CSCwi02134	FTD envoie plusieurs enregistrements NetFlow répliqués pour le même événement de flux
CSCwi02919	SNMP sans réponse lorsque l'hôte du serveur snmp-server est spécifié
CSCwi03528	Accès croisé à l'ifc : rétablissement du protocole PING à l'ancien comportement non croisé à l'ifc
CSCwi06690	Problème d'encodage de certificat lors de l'utilisation de l'authentification/autorisation de certificat AnyConnect
CSCwi07068	SFDataCorrelator consigne « Killing MySQL Connection » (arrêt de la connexion MySQL) chaque minute, ce qui entraîne des problèmes de performance
CSCwi08374	La sauvegarde FMC échoue avec une défaillance « Registration Blocking » (blocage d'enregistrement) causée par des problèmes DCCSM
CSCwi11520	Routage OSPFV3 IPV6 FTD : FTD envoie une demande LSA étendue non prise en charge aux routeurs voisins
CSCwi12284	Vulnérabilité Cisco ASA webvpn
CSCwi12772	Nom du fil de recherche de la source de la grappe ASA : datapath-8-17824
CSCwi13134	Contournement matériel ne fonctionne pas comme prévu dans FP3140.
CSCwi14896	Nœuds expulsés de la grappe lors de l'activation ou de la désactivation du profilage de règle
CSCwi15409	ASA/FTD – recherche de la source et rechargement dans le nom du fil « Unicorn Proxy Thread »
CSCwi15595	ASA recherche de la source et rechargement lors de la modification de la configuration de l'ACL
CSCwi16998	CCM, séq. 58 – LTS18
CSCwi18581	Pare-feu recherche de la source et rechargement en raison du fil SSH
CSCwi19015	ASA/FTD peut rechercher la source et recharger dans le nom de fil « DATAPATH-13-6022 »
CSCwi19145	FTD/ASA peut effectuer une recherche de source et recharger dans PKI, syslog pendant la mise à niveau
CSCwi19849	Chiffrement de grappe d'équilibrage de charge VPN à l'aide de chiffrements obsolètes de phase 2

ID du bogue	En-tête :
CSCwi20114	Vulnérabilité du déni de service SNMP des logiciels Cisco ASA et FTD
CSCwi20848	Utilisation élevée de la mémoire ASA/FTD en raison du protocole SNMP causé par l'interrogation de l'OID RAVPN
CSCwi20955	FTD avec recherche de source possible dans le chemin de données pendant le déploiement lors de l'activation du mode TAP
CSCwi21625	Le mot de passe admin de sécurité intégrée n'est pas correctement synchronisé avec l'activation du contexte du système pw
CSCwi22296	ASA : Le périphérique logique peut démarrer en mode de sécurité intégrée en raison d'une configuration volumineuse.
CSCwi23477	Vulnérabilité de script intersite du logiciel Cisco Firepower Management Center
CSCwi23613	Vulnérabilité d'injection SQL dans Cisco Firepower Management Center
CSCwi24368	Échec de l'ajout du gestionnaire de secours sur le FMC principal en raison d'entrées précédentes dans le tableau
CSCwi24370	Les transactions à haute disponibilité périmées doivent être déplacées vers l'échec et la transaction à haute disponibilité ultérieure doit être créée
CSCwi24461	Périphérique/port-canal tombe en panne avec un cœur généré pour portmanager
CSCwi24880	ASA abandonne le trafic IPSEC incorrectement lorsque « ip verify reverse-path » est configuré
CSCwi26064	ASA : la modification d'une carte de routage dans un contexte affecte les autres contextes
CSCwi26709	Vulnérabilité d'injection HTML du logiciel Cisco Firepower Management Center
CSCwi26895	OID SNMP ASA cpmCPUTotalPhysicalIndex ne renvoyant que des valeurs nulles au lieu des valeurs d'index du CPU
CSCwi27338	Entrée asp périmée pour TCP 443 reste en veille après avoir modifié le port par défaut
CSCwi27402	FTD : Mise à jour du micrologiciel WM à la version 1023.0207
CSCwi27459	Plantage de Snort lors de la sélection de l'algorithme de signature ECDSA
CSCwi28266	Nutanix vFMC n'est pas accessible après la mise à niveau vers la version 7.2.6
CSCwi29934	Vulnérabilité de déni de service du protocole découverte dans la couche de liaison du logiciel Cisco FXOS.
CSCwi31091	La carte de routage de redistribution OSPF avec liste de préfixes ne fonctionne pas après la mise à niveau
CSCwi31766	Le ventilateur du bloc d'alimentation affiche des éléments critiques dans la sortie de l'environnement d'affichage alors qu'il fonctionne normalement

ID du bogue	En-tête :
CSCwi32063	ASA/FTD : Les champs du deuxième facteur du VPN SSL disparaissent
CSCwi32759	L'attribut secondaire du nom d'utilisateur du certificat n'est pas extrait si le premier attribut est manquant
CSCwi34125	ASA : Snmpwalk affiche « No Such Instance » pour l'OID ceSensorExtThresholdValue
CSCwi34719	Impossible de vous connecter en SSH à l'appareil FTD à l'aide de l'authentification extérieure avec RADIUS
CSCwi34730	Le déchiffrement du site Web TLS se rompt avec ERR_HTTP2_PROTOCOL_ERROR
CSCwi35079	Les journaux de mise à niveau de FTD doivent contenir le nom ou les fichiers du certificat
CSCwi35267	TLS1.3 : le décodage du cœur pointe vers tls_trk_try_switch_to_bypass_aux()
CSCwi38061	Recherche de la source et rechargement ASA/FTD en raison d'un dépassement de la limite du descripteur de fichier
CSCwi38957	Échec de l'application de la politique lors du passage de FDM à FMC
CSCwi38962	Vulnérabilité de contournement de la géolocalisation ACL du logiciel Cisco Firepower Threat Defense
CSCwi40487	Échec de la haute disponibilité de FTD après le plantage de SNORT
CSCwi40536	ASA/FTD : Recherche de la source et rechargement lors de l'exécution de l'affichage technique et dans des conditions d'utilisation élevée de la mémoire
CSCwi42295	Le trafic Radius ne passe pas après la mise à niveau de l'ASA 9.18.2 et les versions supérieures.
CSCwi42962	L'installation de la mise à jour du paquet du code de pays GeoDB sur FMC n'envoie pas automatiquement les mises à jour vers les FTD
CSCwi42992	ASA/FTD peut rechercher la source et recharger dans le nom de fil « IKEv2 Daemon »
CSCwi43782	Inspection GTP abandon des paquets avec IE 152 en raison d'une longueur d'en-tête non valide pour IE type 152
CSCwi45630	Recherche de la source Snort3 avec trafics fqdn
CSCwi46010	ASA/FTD : Grappe générant incorrectement le journal système 202010 pour les paquets non valides destinés à l'IP PAT
CSCwi46023	FTD supprime les BPDU à double balise.
CSCwi46641	FTDv peut effectuer une recherche de la source et se recharger dans le nom de fil « PTHREAD-3744 » lors de la modification de l'état de l'interface
CSCwi47288	Vulnérabilité d'injection de commande de sauvegarde de grappe de logiciel Cisco Firepower Management Center

ID du bogue	En-tête :
CSCwi50343	Leur FTD autonome exécutant la version 7.2.2 sur FPR-4112 a fait l'objet d'une recherche de la source sur le module SNMP
CSCwi51941	La mise à niveau FTD en mode sans surveillance de la version 741 à la version 76 échoue si l'ensemble de mise à niveau est déjà copié sur les périphériques
CSCwi53150	Erreur de non-concordance de type de protocole de groupe d'objets de service vue lors du référencement de la liste d'accès déjà
CSCwi53431	Impossible de synchroniser plus de 100 données d'environnement avec l'unité de données
CSCwi56048	File d'attente de fragments d'interface peut être bloquée aux 2/3 de la taille de la base de données de fragments
CSCwi59525	Plusieurs cœurs lina sur 7.2.6 KP2110 géré par cdFMC
CSCwi59831	ASA/FTD peut rechercher la source et recharger dans le nom de fil « lina »
CSCwi62683	Le protocole de transport SSH avec certaines extensions OpenSSH, trouvé dans... (CVE-2023-48795)
CSCwi63844	La politique DNS Umbrella par défaut renvoie une erreur après la mise à niveau vers FMC 7.2.5.1
CSCwi66103	Recherche de la source sur la connexion RAVPN après l'activation du débogage Webvpn
CSCwi67629	Les périphériques peuvent passer à l'état « Manquant le paquet de mise à niveau » après le lancement de la vérification de l'état de préparation
CSCwi68083	Page Mises à niveau de produit : l'action de téléchargement crée de nombreux messages d'erreur « valeur non initialisée » dans le journal
CSCwi71786	Échec du téléchargement pour les paquets de mise à niveau disponibles
CSCwi76002	Épuisement de la mémoire en raison de l'absence du mécanisme de libération pour tmatch
CSCwi76630	FP2100/FP1000 : Licences Smart pour ASA perdues après le rechargement
CSCwi79703	Format de fuseau horaire incorrect sur FTD lors de la configuration par FXOS
CSCwi80465	CCM ID 63 - LTS18
CSCwi86198	Le corrélateur SFDData continue de se terminer sur les FTD configurés pour les IDS
CSCwi90040	Vulnérabilité d'injection de commande des logiciels Cisco ASA et FTD
CSCwi90371	ASA : demande d'ajouter l'option « logging list » (liste de journalisation) à la commande « logging history »
CSCwi95708	FTD : nom d'hôte manquant dans le message Syslog

ID du bogue	En-tête :
CSCwi98284	Vulnérabilité d'exécution de code local persistante des logiciels Cisco ASA et FTD
CSCwj02708	La génération de la sauvegarde sur FDM échoue avec l'erreur « Impossible de sauvegarder les données existantes »
CSCwj10955	Vulnérabilité de déni de service des services Web des logiciels Cisco ASA et FTD
CSCwj16633	Problèmes liés à l'aperçu du déploiement de FMC (aperçu avancé)
CSCwk84221	FPR3100 : interfaces SFP 25G ne se déclenchent pas après le redémarrage

Bogues résolus dans la version 7.2.5.2

Dernière mise à jour du tableau : 06/05/2024

Tableau 32 : Bogues résolus dans la version 7.2.5.2

ID du bogue	En-tête :
CSCwe41766	FTD peut ne pas redémarrer comme prévu après la mise à niveau si la version FXOS groupée est la même sur l'ancienne et la nouvelle version
CSCwi90040	Vulnérabilité d'injection de commande des logiciels Cisco ASA et FTD
CSCwi98284	Vulnérabilité d'exécution de code local persistante des logiciels Cisco ASA et FTD
CSCwj10955	Vulnérabilité de déni de service des services Web des logiciels Cisco ASA et FTD

Bogues résolus dans la version 7.2.5.1

Tableau mis à jour le : 25/02/2025

Tableau 33 : Bogues résolus dans la version 7.2.5.1

ID du bogue	En-tête :
CSCvt25221	Recherche de la source FTD dans le nom du fil cli_xml_server lors du déploiement de la politique QoS
CSCvx04003	Le manque de limitation des indicateurs manqués d'ARP au CP entraîne un surabonnement
CSCwc51588	Échec de la génération de la sauvegarde/restauration FMC par SMB/SSH
CSCwc62215	FTD n'a pas pu synchroniser la haute disponibilité en raison d'un échec de validation du SNORT
CSCwc78781	ASA/FTD peut effectuer une recherche de la source et se recharger pendant les modifications d'ACL liées à la configuration PBR
CSCwc82205	ASA/FTD peut rechercher la source et recharger dans le nom de fil « lina »

ID du bogue	En-tête :
CSCwe99053	FDM : La commande « réplication de basculement http » peut disparaître de la configuration en cours d'exécution de FTD
CSCwd27186	Tout le trafic bloqué en raison d'une commande access-group manquante dans la configuration FTD
CSCwd38196	Le serveur mandataire est activé même lorsque nous avons une règle DND définitive
CSCwd38583	ASA/FTD : Commande « no snmp-server enable oid mempool » activée par défaut ou appliquée lors des mises à niveau
CSCwd86535	ASA/FTD : Recherche de la source et rechargement sur la minuterie NetFlow infra
CSCwd89095	Port SFP membre du canal LACP Stratix5950 et ISA3000 suspendu après le rechargement
CSCwe04043	La mise à niveau de la haute disponibilité de FTD échoue en raison du démarrage de la mise à niveau d'une unité avant que l'autre ne rejoigne la paire de haute disponibilité
CSCwe12705	Recherche de la source multimode-tmatch_df_kijack_walk observé lors de l'arrêt ou de la désactivation sur l'interface du commutateur connecté à FO
CSCwe18090	Échec du déploiement de FMC : « Échec de la validation : il s'agit d'un périphérique de secours slave*/ha, rejetant le déploiement ».
CSCwe18216	Erreur de connexion nulle vue dans les journaux
CSCwe28407	Recherche de la source LINA avec icmp_thread
CSCwe37132	L'identité du serveur TLS peut pousser certains clients à produire un message Hello du client altéré
CSCwe37453	La passerelle n'est pas accessible à partir de l'unité de secours dans le contexte de l'administrateur et de l'utilisateur avec une interface de gestion partagée
CSCwe38029	Recherche de la source multiple vue sur l'unité de secours.
CSCwe39546	FMC : la sauvegarde vers un hôte distant non disponible entraîne l'impossibilité de redémarrer le périphérique.
CSCwe42061	La suppression d'un BVI dans les interfaces FTD entraîne des abandons de paquets dans les autres BVI.
CSCwe44571	FMC : La taille de la géolocalisation entraîne des échecs de mise à niveau
CSCwe47671	Utilisation élevée de la mémoire sur monetDB, FMC n'affiche pas les événements de connexion
CSCwe51443	Évaluation ASA de la vulnérabilité OpenSSL CVE-2022-4450
CSCwe55298	La politique DNS Umbrella ne prend pas en compte plusieurs URL saisies dans le champ de domaine de contournement

ID du bogue	En-tête :
CSCwe74089	ASA/FTD peut rechercher la source et recharger dans le nom de fil « DATAPATH-1-1656 »
CSCwe79051	Le déploiement pour la modification eigrp/bgp peut entraîner une panne temporaire pendant l'application de la politique
CSCwe82704	Les sous-interfaces PortChannel configurées en tant que partage de données/données, dans la haute disponibilité d'instances multiples passent en « attente »
CSCwe83255	ASA/FTD peut rechercher la source et recharger dans le nom de fil « lina »
CSCwe90609	Vulnérabilité du déni de service SNMP des logiciels Cisco ASA et FTD
CSCwe90720	Recherche de la source et rechargement ASA dans le fil d'analyse en raison de la corruption ha_msg
CSCwe92905	Le processus ngfwManager redémarre continuellement, entraînant un retour en arrière de mémoire pour ZMQ
CSCwe93176	Affectations de règles Snort2 manquantes dans ngfw.rules (assignment_data_table) après la mise à niveau de FMC
CSCwe99550	Ajouter un bouton pour suspendre/reprendre la journalisation spécifique au fichier dans asa log infra.
CSCwf04870	ASA : « Ping<ifc_name> x.x.x.x » ne fonctionne pas comme prévu à partir de la version 9.18.x
CSCwf05295	FTD exécuté sur la série FP1000 peut abandonner les paquets sur les flux TLS après le message « Client Hello ».
CSCwf10910	FTD : Recherche de la source dans ZMQ en cours d'exécution 7.3.0
CSCwf12005	ASA envoie une demande OCSP sans agent utilisateur ni hôte
CSCwf12985	FTDv : Défaillance du trafic dans les déploiements VMware en raison de l'épuisement du pool dpdk et de rx_buff_alloc_failure
CSCwf14126	Recherche de la source et rechargement d'ASA sur le nom de processus Lina
CSCwf15858	L'authentification LDAP sur SSL ne fonctionne pas pour les utilisateurs qui envoient des profils d'autorisation volumineux
CSCwf15902	ASAv dans Hyper-V abandonne les paquets sur l'interface de gestion
CSCwf16559	La demande pjb d'état de préparation est très fréquente lorsque l'utilisateur est dans la page de liste de capteurs de mise à niveau
CSCwf17042	ASDM remplace la carte de politiques personnalisée par une carte par défaut sur les options d'inspection de classe lors de la restauration de la sauvegarde.
CSCwf17406	Échec de la suppression des fichiers de statistiques snort antérieurs à 70 jours

ID du bogue	En-tête :
CSCwf20338	ASA peut rechercher la source et recharger dans le nom de fil « DHCPv6 Relay »
CSCwf23262	Vulnérabilité de contournement de la liste de contrôle d'accès Cisco ASA et FTD AnyConnect
CSCwf26407	FP2130- Impossible de dissocier le membre du canal de port, échec du déploiement, le membre est perdu sur FTD/FMC
CSCwf26534	Appareil de sécurité adaptable (ASA)/Protection contre les menaces Firepower (FTD) : Les informations de connexion dans l'en-tête SIP-SDP restent non traduites avec une destination statique Any
CSCwf30716	Appareil de sécurité adaptable dans le contexte multiple affiche le périphérique en veille dans l'état défaillant même après la récupération de MIO HB.
CSCwf31701	Recherche de la source de l'appareil de sécurité adaptable et rechargement avec le nom du fil : « CP Crypto Result Processing »
CSCwf34152	FMC ne parvient pas à déployer ou à enregistrer de nouveaux FTD en raison d'un échec de l'établissement de SFTunnel.
CSCwf34500	Protection contre les menaces Firepower : Le trafic GRE n'est pas équilibré en charge entre les cœurs de CPU
CSCwf35207	Appareil de sécurité adaptable : recherche de la source et rechargement lors de la mise à jour des listes de contrôle d'accès sur l'Appareil de sécurité adaptable
CSCwf35233	DoS du logiciel de l'Appareil de sécurité adaptable et de Firepower Threat Defense
CSCwf35573	Le trafic peut être affecté si le délai d'expiration de la sonde d'identité du serveur TLS est trop long
CSCwf36563	La configuration de l'interface est manquante après la mise à niveau de FTD
CSCwf37160	Échec de connexion AnyConnect Ikev2 avec mappage de groupe de certificats configuré
CSCwf42144	ASA/FTD peut rechercher la source et recharger en indiquant le nom de processus « lina »
CSCwf43288	Recherche de la source dans le nom du fil : ssh/client dans une configuration en grappe
CSCwf43537	Plantage de lina dans le nom du fil : cli_xml_request_process lors de la mise à niveau de la grappe FTD
CSCwf44537	Plantage de lina 99.20.1.16 sur nat_remove_policy_from_np
CSCwf47227	Retirer la commande Priority-queue de FTD La commande Priority-queue entraîne des abandons de paquets de sortie silencieux
CSCwf48599	Chiffrement de grappe d'équilibrage de charge VPN à l'aide de chiffrements obsolètes
CSCwf49486	La tâche store_*list_history.pl est créée toutes les 5 minutes sans être fermée, ce qui entraîne une lenteur du FMC.

ID du bogue	En-tête :
CSCwf49573	ASA/FTD : Recherche de la source et rechargement lors de l'émission « show memory webvpn all objects »
CSCwf50497	L'épuisement des entrées de cache DNS entraîne une recherche de la source
CSCwf54510	Recherche de la source et rechargement pour le nom du fil : DHCPRA Monitor
CSCwf56386	vFTD manque de mémoire et passe à l'état d'échec
CSCwf56811	Recherche de la source ASA et rechargement sur le nom du processus lina en raison de la validation de l'en-tête de mémoire
CSCwf58876	KP2140-HA, unité principale rechargée n'est pas en mesure de détecter l'unité homologue
CSCwf60311	ASA générant une recherche de la source avec le nom du fil : DATAPATH-53-18309 après la mise à niveau à la version 9.16.4.19
CSCwf60590	« show route all summary » exécuté en mode transparent sur FTD fait de CLISH un lent.
CSCwf62729	Vulnérabilité du déni de service SSL/TLS de Cisco ASA/FTD Firepower 2100
CSCwf62820	Basculement : recherche de la source et rechargement de l'unité de secours lors de la modification des listes d'accès
CSCwf69901	FTD : Recherche de la source et rechargement pendant l'exécution du processus de redistribution OSPF
CSCwf71812	Le moteur FTD Lina peut effectuer une recherche de source en raison d'une assertion dans le chemin de données
CSCwf72434	Ajouter des journaux significatifs lorsque les règles de limite maximale du système sont atteintes
CSCwf77191	En mode appareil ASA – « connect fxos [admin] » obtiendra une erreur : échec de l'ouverture de la connexion
CSCwf78321	ASA : Recherche de la source et rechargement en raison d'un WebVPN sans client
CSCwf81058	FTD : déchargement de flux dynamique du Firepower 3100 affiché comme activé
CSCwf82247	Le déploiement de la stratégie échoue lorsqu'une route même préfixe/métrique est configurée dans un VRF distinct.
CSCwf82742	Cisco FTD : SNMP ne fonctionne pas sur l'interface de gestion
CSCwf82970	Le moteur Snort2 plante après l'activation de la fonction de découverte de l'identité du serveur TLS
CSCwf92135	ASA : Recherche de la source et rechargement sur le nom de fil « fover_FSM_thread » et ha_ntpy_prog_process_timer

ID du bogue	En-tête :
CSCwf92182	Vulnérabilité d'injection SQL du logiciel Cisco Firepower Management Center
CSCwf92646	Certificat autosigné ECDSA utilisant SHA384 pour EC521
CSCwf92726	Certains secrets de Vault, y compris les fichiers LDAP manquants après la mise à niveau si le jeton de Vault est corrompu
CSCwf95147	Le trafic OSPFv3 est centralisé en mode transparent
CSCwf96938	FMC : La règle ACP avec le port UDP 6081 est supprimée après le déploiement ultérieur
CSCwh01673	Espace disque FTD/ngfw complet à partir des fichiers db d'URL Snort3
CSCwh02457	L'authentification Radius a cessé de fonctionner après la mise à niveau de l'ASAv sur AWS vers une version ultérieure à la version 9.18.2
CSCwh04231	FMC doit maintenir correctement le répertoire de données Redis pour éviter une utilisation non liée du disque
CSCwh04365	Recherche de la source ASA et rechargement sur le nom du processus lina en raison de la validation de l'en-tête de mémoire - correctif côté webvpn
CSCwh04395	L'application ASDM se termine de manière aléatoire ou se termine avec un message d'alerte sur la configuration multi-contexte
CSCwh11764	ASA/FTD peut effectuer la recherche de la source et se recharger dans le nom de fil « RAND_DRBG_bytes » et la fonction CTM sur les plateformes n5
CSCwh12987	Les serveurs SMB de grande taille entraînent l'expiration du délai de renvoi des verdicts entre les périphériques FMC et FTD
CSCwh14467	Les tailles de fichiers supérieures à 100 Mo pour les images AnyConnect/Secure Client ne peuvent pas être chargées sur FMC
CSCwh14584	Recherche de la source vue sur FTD fonctionnant sur la gamme Firepower 2100
CSCwh14597	ASA/FTD sans résidu
CSCwh15223	Plantage de Lina dans snp_fp_tcp_normalizer() lorsque DAQ/Snort envoie un en-tête L3 malformé
CSCwh21141	Le déploiement de l'aperçu de FMC affiche des informations incorrectes.
CSCwh23100	Vulnérabilité d'accès non autorisé aux logiciels Cisco ASA et FTD
CSCwh23567	Fichier de clé PAC manquant en veille lors du rechargement
CSCwh26526	Les paquets SQL impliqués dans une grande requête sont abandonnés par SNORT3 avec le motif snort-block
CSCwh27230	Les connexions ne sont pas effacées après le délai d'inactivité lorsque les interfaces sont en mode en ligne.

ID du bogue	En-tête :
CSCwh28144	L'OID spécifique 1.3.6.1.2.1.25 ne devrait pas répondre
CSCwh30891	ASA/FTD peut effectuer une recherche de la source et se recharger dans le nom de fil « ssh » lors de l'ajout de la configuration SNMPV3
CSCwh32118	Limite de sessions de gestion ASDM atteinte en raison de sessions HTTP bloquées dans CLOSE_WAIT
CSCwh36005	Le déploiement de la politique a échoué en raison de « 1 erreurs observées lors de populateGlobalSnapshot »
CSCwh37733	FTD répond au paquet UDP500 avec l'adresse MAC 0000.000.000
CSCwh40968	Échec du téléchargement d'un fichier volumineux en raison d'une limite maximale de segments
CSCwh41127	ASA/FTD : Erreur NAT64 « chevauche l'adresse de l'interface de secours interne » pour l'ASA autonome
CSCwh45108	Vulnérabilité d'accès non autorisé aux logiciels Cisco ASA et FTD
CSCwh49483	ASA/FTD peut effectuer une recherche de source et se recharger pendant l'exécution de l'inventaire
CSCwh52420	Le délai de recherche dans le nuage AMP expire fréquemment.
CSCwh56945	SFDataCorrelator plante sans arrêt dans ARN_DB_InsertServiceInfo
CSCwh58999	Échec de l'enregistrement des périphériques avec des licences classiques auprès de FMC exécutant la version 7.2.X
CSCwh64508	Correction de la rétrogradation entraînée lors du traitement de l'interface utilisateur Web n'obtient pas la variable FTDv
CSCwh69209	Le préfiltre ne peut pas ajouter de points terminaux au tunnel dans la règle de tunnel sur FMC
CSCwh69815	Le débit des FTDv a été modifié à 100 kbit/s après la mise à niveau
CSCwi82368	Les licences classiques doivent être ajoutées manuellement après l'enregistrement pour obtenir une licence pendant la migration/l'autorisation de retour de matériel
CSCwi90040	Vulnérabilité d'injection de commande des logiciels Cisco ASA et FTD
CSCwi98284	Vulnérabilité d'exécution de code local persistante des logiciels Cisco ASA et FTD
CSCwj10955	Vulnérabilité de déni de service des services Web des logiciels Cisco ASA et FTD
CSCwj42876	DOC Impossible d'ajouter une licence SLR sur la haute disponibilité de FMC.
CSCwj56796	DOC : Ajout d'une section sur les bogues résolus pour le correctif 7.2.5.1
CSCwk25371	LOM est pris en charge sur le port CIMC dans FMC4600, mais certains documents indiquent qu'il n'est disponible que sur eth0

Bogues résolus dans la version 7.2.5

Dernière mise à jour du tableau : 22-05-2024

Tableau 34 : Bogues résolus dans la version 7.2.5

ID du bogue	En-tête :
CSCvo60131	Les enregistrements du journal d'audit ne s'affichent pas dans le bon ordre
CSCwb08189	Le trafic de mise à jour de Microsoft bloqué avec l'inspection de programmes malveillants Snort version 3
CSCwb95453	ASA : L'horodatage de tous les journaux générés par le contexte Admin est le même
CSCwb95784	Mettre en cache et vidanger les 20 derniers paquets de réponse à la demande rmu en cas de défaillance ou de retard lors de la lecture des registres
CSCwd14732	FTD Impossible de se lier au port 8305 après la modification de l'IP de gestion
CSCwd16850	Des renseignements supplémentaires sont requis dans les messages du journal système 202010 pour effectuer le dépannage
CSCwd34888	FP1000 - Pendant le processus de démarrage en mode LINA, il y a eu des fuites de diffusions entre les interfaces, ce qui a provoqué une tempête
CSCwd41224	Interface utilisateur Web à haute disponibilité du FMC ne reçoit pas le niveau de variable FTDv affecté à FTDv - Variable
CSCwd67101	FPR1150 : Erreur de format d'exécution constatée et appareil bloqué jusqu'au rechargement, après exécution de « secure all »
CSCwd94181	Non affichage de la lame après la mise à jour de FXOS pour instances multiples en raison d'un problème de rotation du journal ssp_ntp.log
CSCwe03529	Recherche de la source et rechargement FTD lors du déploiement de PAT POO
CSCwe06562	FPR1K/FPR2K : Augmentation du temps de basculement en mode transparent avec un nombre élevé de sous-interfaces
CSCwe07722	L'unité de données de grappe abandonne le trafic non VPN avec la raison ASP « Échec de reclassification du VPN »
CSCwe21187	ASA/FTD peut abandonner les paquets de multidiffusion en raison d'une raison d'abandon de l'ASP no-mcast-intrf jusqu'à l'expiration du délai UDP
CSCwe21280	Les messages syslog de connexion ou de démontage de multidiffusion peuvent ne pas toujours être générés
CSCwe23801	FPR2100 : Plusieurs cœurs snort3 et snort2 ont été générés et le capteur tombe en panne dans la plateforme KP
CSCwe29529	Le MI FTD n'ajuste pas le PVID sur les vlans reliés aux BVI

ID du bogue	En-tête :
CSCwe30567	Solution de contournement pour définir hwclock à partir des journaux de ntp sur les plates-formes bas de gamme
CSCwe44672	Le journal système ASA-6-611101 est généré deux fois pour une seule connexion ssh
CSCwe45569	La mise à niveau de FTD de la version 7.0 à la version 7.2.x et au-delà se bloque en raison de l'accès de gestion activé
CSCwe45653	Amélioration : FXOS doit effectuer le suivi du problème lié au dépassement du quota de disque du module Security
CSCwe50993	SNMP sur le module SFR s'éteint et ne se rallume pas
CSCwe51286	ASA/FTD peut rechercher la source et recharger dans le nom de fil « lina »
CSCwe52120	Les connexions SSL déchiffrées échouent lorsque tx chksum-offload est activé avec l'interface de sortie un ppoe.
CSCwe54529	FTD sur FPR2140 – Recherche de la source sur la ligne et rechargement par normalisation TCP
CSCwe54567	Le gestionnaire se désenregistre de lui-même du FTD, afficher gestionnaire affiche « Aucun gestionnaire configuré »
CSCwe58881	Après la mise à niveau de FMC, le ruban SecureX redirige vers la région du nuage des États-Unis, quelle que soit la région du nuage définie
CSCwe59737	L'ASA/FTD redémarre en raison d'une recherche de la source pointant vers un délai d'attente de surveillance sur p3_tree_lookup
CSCwe61928	Les paquets de registre PIM ne sont pas envoyés au RP après un rechargement si FTD utilise une passerelle par défaut pour atteindre le RP
CSCwe61969	Attribut d'interface ASA multicontexte « gestion uniquement » non synchronisé lors de la création
CSCwe62703	Les nouvelles sous-commandes de contexte ne sont pas répliquées en mode veille à haute disponibilité lorsque plusieurs sessions sont ouvertes.
CSCwe63067	ASA/FTD peut effectuer une recherche de la source et se recharger dans le nom de fil « lina » en raison de l'état d'interception TCP
CSCwe63316	Pri-Active FMC ne déclenche PAS l'enregistrement de la tâche pour que FTD configure le gestionnaire en veille
CSCwe64043	Listes de contrôle d'accès Cisco ASA et FTD non installées lors du rechargement
CSCwe65634	ASA – Le périphérique en veille peut effectuer une recherche de source et se recharger pendant la synchronisation d'ACL DAP
CSCwe67751	Le dernier fragment des paquets SIP IPv6 a un MF égal à 1, indiquant que d'autres paquets sont attendus

ID du bogue	En-tête :
CSCwe67816	Recherche de la source ASA/FTD et rechargement lors du retrait de la capture d'isakmp
CSCwe68159	Le fichier de basculement fover_trace.log est inondé et est remplacé rapidement
CSCwe68917	Snort3 ne parvient pas à faire correspondre le trafic SMTPS aux règles ACP
CSCwe70202	Plusieurs fois, le basculement peut être désactivé en voyant par erreur un autre « mode opérationnel de soutien ».
CSCwe74916	L'interface reste HORS-SERVICE dans un ensemble Inline avec propagation de l'état du lien.
CSCwe76722	ASA/FTD : Échec de la connexion Ping à partir de la boîte lors de l'utilisation d'un VRF personnalisé
CSCwe78977	ASA/FTD peut effectuer une recherche de la source et un rechargement dans le nom de fil « pix_flash_config_thread »
CSCwe79072	ASA/FTD peut rechercher la source et recharger dans le nom de fil « lina »
CSCwe81684	ASA : Défaillance en veille lors de l'analyse de « management-only » non signalée au sous-système d'analyse ou de basculement
CSCwe85432	Recherche de la source ASA/FTD et rechargement sur le fil DATAPATH-14-11344 lorsque l'inspection SIP est activée
CSCwe88772	Recherche de la source et rechargement de l'appareil de sécurité adaptable avec le nom du processus : cli_xml_request_process
CSCwe90202	ASA : Défaillance en veille lors de l'analyse de « management-only » (gestion uniquement) pour les modifications de configuration dynamique
CSCwe90334	ID d'instance manquant dans unified_events-2.log
CSCwe93532	ASA/FTD peut effectuer une recherche de la source et se recharger dans le nom de fil « lina »
CSCwe93537	La détection des menaces ne permet pas d'effacer les entrées IPv6 individuelles
CSCwe94287	Le relais DHCP FTD abandonne la NACK si plusieurs serveurs DHCP sont configurés
CSCwe95729	Vulnérabilité de contournement de l'authentification Cisco ASA et FTD SAML
CSCwe95757	ASA/FTD peut rechercher la source et recharger dans le nom de fil « lina »
CSCwe96023	ASA/FTD : Recherche de la source associée à SNMP et rechargement immédiatement après la mise à niveau de la version 6.6.5 à la version 7.0.1
CSCwe96068	ASA : CLU configurable pour un grand nombre de sous-débits/dépassements sur les files d'attente RX/TX CLU
CSCwe99040	recherche de la source et rechargement du chemin de données de fil sur le processus tcpmod_proxy_continue_bp

ID du bogue	En-tête :
CSCwf00417	FTD : Impossible de traiter un site Web TLS1.2 avec une identité de serveur TLS avec des erreurs SSL générées par le client
CSCwf00865	Le VPN FTD/ASA concentrateur et en étoile (U-turn) échoue lorsqu'une étoile est chargée dans un flux IPSec et que l'autre ne l'est pas
CSCwf01064	Le protocole Ping TCP est complètement interrompu à partir de la version 9.18.2
CSCwf02363	Plantage Snort3 dans SslServiceDetector après l'appel de nss_passwd_lookup
CSCwf03490	portmanager.sh affiche les avertissements bash continus dans les fichiers journaux
CSCwf04831	ASA/FTD peut rechercher la source et recharger dans le nom de fil 'ci/console'
CSCwf07791	ASA à court de fragments SNMP PDU et SNMP VAR
CSCwf08043	Recherche de la source et rechargement de Lina en raison de paquets fragmentés
CSCwf08515	FPR3100 : Impact élevé du trafic des appareils de sécurité adaptables Cisco/Cisco FTD sur toutes les interfaces de données avec un nombre élevé de « demux drops »
CSCwf10486	Filtre de réseau d'intégration ISE n'acceptant pas plusieurs réseaux séparés par des virgules
CSCwf12408	ASA : Après la mise à niveau vers la version 9.16.4, tous les mots de passe de type 8 sont perdus lors du premier redémarrage
CSCwf14735	recherche de la source et rechargement dans le nom du processus : lina lié à la NAT/Pat
CSCwf14811	Le normalisateur TCP a besoin de statistiques qui affichent des actions telles que les pertes de paquets
CSCwf17814	ASA/FTD peut rechercher la source et recharger dans le nom de fil '19', échec de la somme de contrôle du blocage libre
CSCwf21106	ASA/FTD : Recherche de la source sur le nom du fil : snmp_master_callback_thread pendant les modifications de SNMP et d'interface
CSCwf22045	MYSQL, ou tout trafic TCP élevé, bloqué par snort3, avec snort-block comme raison d'abandon
CSCwf23564	Impossible d'établir BGP lors de l'utilisation de l'authentification MD5 sur le TUNNEL GRE et de FTD comme appareil d'intercommunication
CSCwf24124	Le processus SFDataCorrelator se bloque très fréquemment sur le FMC.
CSCwf24773	crashhandler exécuté avec le mode de test snort
CSCwf26939	FTD peut ne pas créer de règle NAT avec l'erreur suivante : « IPv4 dst real obj address range is huge »
CSCwf28488	Messages de journal incohérents vus lorsque l'indicateur est configuré et que la journalisation de la mémoire tampon est définie sur débogage

ID du bogue	En-tête :
CSCwf28592	Dans certains scénarios spécifiques, l'optimiseur d'objets peut entraîner le déploiement de règles incorrectes sur le périphérique
CSCwf30727	L'intégration de l'appareil de sécurité adaptable avec Cisco Umbrella ne fonctionne pas sans utilisation de validation ssl-server.
CSCwf31820	Le pare-feu peut abandonner des paquets lors du routage entre les VRFs globaux ou d'utilisateur
CSCwf33574	Les entrées de liste d'accès ASA ont le même hachage après la mise à niveau
CSCwf34450	Plantage de Snort3 après le redémarrage de Snort si des applications personnalisées en double sont présentes
CSCwf35510	Segfault possible dans Snort3 lorsque appid tente de supprimer la table d'informations sur l'application
CSCwf51933	Échec de connexion par authentification extérieure pour le AAA-RADIUS après la mise à niveau
CSCwf54418	Réduire le temps nécessaire pour effacer les SA IKEv2 périmées formées après la détection en double
CSCwf60584	Surveillance de l'intégrité pour ne pas collecter les statistiques de routage pour le mode transparent FTD
CSCwf62885	Le mandataire à une seule branche FTDv derrière AWS GWLB abandonne en raison d'une somme de contrôle geneve-invalid-udp-checksum.
CSCwf71606	Listes de contrôle d'accès Cisco ASA et FTD non installées lors du rechargement
CSCwf73189	Cisco FTD abandonne le trafic GRE de WSA en raison d'une défaillance de la NAT
CSCwf76945	Les données des paquets sont toujours abandonnées après la mise à niveau
CSCwf85307	Les remplacements de politique IPS [Snort 3] ne fonctionnent pas sur les politiques de prévention des intrusions en chaîne
CSCwf88552	ASA/FTD : Recherche de la source et rechargement en raison de la réécriture de l'inspection NAT L7
CSCwf99173	DOC : Lors de l'utilisation d'un SLR, il n'est pas correctement documenté ce qui se passe si l'une des licences expire.
CSCwh01154	FTD : les interfaces complètes/10 Gbps ont été remplacées par 1 Gbit/s/auto après la mise à niveau et l'état d'arrêt

Bogues résolus dans la version 7.2.4.1

Dernière mise à jour du tableau : 22-05-2024

Tableau 35 : Bogues résolus dans la version 7.2.4.1

ID du bogue	En-tête :
CSCvo60131	Les enregistrements du journal d'audit ne s'affichent pas dans le bon ordre
CSCwb08189	Le trafic de mise à jour de Microsoft bloqué avec l'inspection de programmes malveillants Snort version 3
CSCwb95453	ASA : L'horodatage de tous les journaux générés par le contexte Admin est le même
CSCwd14732	FTD Impossible de se lier au port 8305 après la modification de l'IP de gestion
CSCwd16850	Des renseignements supplémentaires sont requis dans les messages du journal système 202010 pour effectuer le dépannage
CSCwd34888	FP1000 - Pendant le processus de démarrage en mode LINA, il y a eu des fuites de diffusions entre les interfaces, ce qui a provoqué une tempête
CSCwd41224	Interface utilisateur Web à haute disponibilité du FMC ne reçoit pas le niveau de variable FTDv affecté à FTDv - Variable
CSCwd67101	FPR1150 : Erreur de format d'exécution constatée et appareil bloqué jusqu'au rechargement, après exécution de « secure all »
CSCwd94181	Non affichage de la lame après la mise à jour de FXOS pour instances multiples en raison d'un problème de rotation du journal ssp_ntp.log
CSCwe03529	Recherche de la source et rechargement FTD lors du déploiement de PAT POO
CSCwe06562	FPR1K/FPR2K : Augmentation du temps de basculement en mode transparent avec un nombre élevé de sous-interfaces
CSCwe07722	L'unité de données de grappe abandonne le trafic non VPN avec la raison ASP « Échec de reclassification du VPN »
CSCwe21187	ASA/FTD peut abandonner les paquets de multidiffusion en raison d'une raison d'abandon de l'ASP no-mcast-intrf jusqu'à l'expiration du délai UDP
CSCwe21280	Les messages syslog de connexion ou de démontage de multidiffusion peuvent ne pas toujours être générés
CSCwe29529	Le MI FTD n'ajuste pas le PVID sur les vlans reliés aux BVI
CSCwe30567	Solution de contournement pour définir hwclock à partir des journaux de ntp sur les plates-formes bas de gamme
CSCwe44672	Le journal système ASA-6-611101 est généré deux fois pour une seule connexion ssh
CSCwe45653	Amélioration : FXOS doit effectuer le suivi du problème lié au dépassement du quota de disque du module Security

ID du bogue	En-tête :
CSCwe50993	SNMP sur le module SFR s'éteint et ne se rallume pas
CSCwe51286	ASA/FTD peut rechercher la source et recharger dans le nom de fil « lina »
CSCwe52120	Les connexions SSL déchiffrées échouent lorsque tx chksum-offload est activé avec l'interface de sortie un pppoe.
CSCwe54529	FTD sur FPR2140 – Recherche de la source sur la ligne et rechargement par normalisation TCP
CSCwe54567	Le gestionnaire se désenregistre de lui-même du FTD, afficher gestionnaire affiche « Aucun gestionnaire configuré »
CSCwe58881	Après la mise à niveau de FMC, le ruban SecureX redirige vers la région du nuage des États-Unis, quelle que soit la région du nuage définie
CSCwe59737	L'ASA/FTD redémarre en raison d'une recherche de la source pointant vers un délai d'attente de surveillance sur p3_tree_lookup
CSCwe61928	Les paquets de registre PIM ne sont pas envoyés au RP après un rechargement si FTD utilise une passerelle par défaut pour atteindre le RP
CSCwe61969	Attribut d'interface ASA multicontexte « gestion uniquement » non synchronisé lors de la création
CSCwe62703	Les nouvelles sous-commandes de contexte ne sont pas répliquées en mode veille à haute disponibilité lorsque plusieurs sessions sont ouvertes.
CSCwe63067	ASA/FTD peut effectuer une recherche de la source et se recharger dans le nom de fil « lina » en raison de l'état d'interception TCP
CSCwe63316	Pri-Active FMC ne déclenche PAS l'enregistrement de la tâche pour que FTD configure le gestionnaire en veille
CSCwe64043	Listes de contrôle d'accès Cisco ASA et FTD non installées lors du rechargement
CSCwe65634	ASA – Le périphérique en veille peut effectuer une recherche de source et se recharger pendant la synchronisation d'ACL DAP
CSCwe67751	Le dernier fragment des paquets SIP IPv6 a un MF égal à 1, indiquant que d'autres paquets sont attendus
CSCwe67816	Recherche de la source ASA/FTD et rechargement lors du retrait de la capture d'isakmp
CSCwe68159	Le fichier de basculement fover_trace.log est inondé et est remplacé rapidement
CSCwe68917	Snort3 ne parvient pas à faire correspondre le trafic SMTPS aux règles ACP
CSCwe70202	Plusieurs fois, le basculement peut être désactivé en voyant par erreur un autre « mode opérationnel de soutien ».
CSCwe74916	L'interface reste HORS-SERVICE dans un ensemble Inline avec propagation de l'état du lien.

ID du bogue	En-tête :
CSCwe76722	ASA/FTD : Échec de la connexion ping à partir de la boîte lors de l'utilisation d'un VRF personnalisé
CSCwe78977	ASA/FTD peut effectuer une recherche de la source et un rechargement dans le nom de fil « pix_flash_config_thread »
CSCwe79072	ASA/FTD peut rechercher la source et recharger dans le nom de fil « lina »
CSCwe81684	ASA : Défaillance en veille lors de l'analyse de « management-only » non signalée au sous-système d'analyse ou de basculement
CSCwe85432	Recherche de la source ASA/FTD et rechargement sur le fil DATAPATH-14-11344 lorsque l'inspection SIP est activée
CSCwe88772	Recherche de la source et rechargement de l'appareil de sécurité adaptable avec le nom du processus : cli_xml_request_process
CSCwe90202	ASA : Défaillance en veille lors de l'analyse de « management-only » (gestion uniquement) pour les modifications de configuration dynamique
CSCwe90334	ID d'instance manquant dans unified_events-2.log
CSCwe93532	ASA/FTD peut effectuer une recherche de la source et se recharger dans le nom de fil « lina »
CSCwe93537	La détection des menaces ne permet pas d'effacer les entrées IPv6 individuelles
CSCwe94287	Le relais DHCP FTD abandonne la NACK si plusieurs serveurs DHCP sont configurés
CSCwe95729	Vulnérabilité de contournement de l'authentification Cisco ASA et FTD SAML
CSCwe95757	ASA/FTD peut rechercher la source et recharger dans le nom de fil « lina »
CSCwe96023	ASA/FTD : Recherche de la source associée à SNMP et rechargement immédiatement après la mise à niveau de la version 6.6.5 à la version 7.0.1
CSCwe96068	ASA : CLU configurable pour un grand nombre de sous-débits/dépassements sur les files d'attente RX/TX CLU
CSCwe99040	recherche de la source et rechargement du chemin de données de fil sur le processus tepmod_proxy_continue_bp
CSCwf00417	Impossible de traiter un site Web TLS1.2 avec une identité de serveur TLS, il génère ERR_SSL_PROTOCOL_ERROR.
CSCwf00865	Le VPN FTD/ASA concentrateur et en étoile (U-turn) échoue lorsqu'une étoile est chargée dans un flux IPSec et que l'autre ne l'est pas
CSCwf01064	Le protocole Ping TCP est complètement interrompu à partir de la version 9.18.2
CSCwf02363	Plantage Snort3 dans SslServiceDetector après l'appel de nss_passwd_lookup
CSCwf03490	portmanager.sh affiche les avertissements bash continus dans les fichiers journaux

ID du bogue	En-tête :
CSCwf04831	ASA/FTD peut rechercher la source et recharger dans le nom de fil 'ci/console'
CSCwf06818	Vulnérabilité de contournement de la politique de fichiers d'archive chiffrée du logiciel Cisco Firepower Threat Defense
CSCwf07791	ASA à court de fragments SNMP PDU et SNMP VAR
CSCwf08043	Recherche de la source et rechargement de Lina en raison de paquets fragmentés
CSCwf08515	FPR3100 : Impact élevé du trafic des appareils de sécurité adaptables Cisco/Cisco FTD sur toutes les interfaces de données avec un nombre élevé de « demux drops »
CSCwf10486	Filtre de réseau d'intégration ISE n'acceptant pas plusieurs réseaux séparés par des virgules
CSCwf12408	ASA : Après la mise à niveau vers la version 9.16.4, tous les mots de passe de type 8 sont perdus lors du premier redémarrage
CSCwf14735	Recherche de la source et rechargement dans le nom du processus : lina lié à la NAT/Pat
CSCwf14811	Le normalisateur TCP a besoin de statistiques qui affichent des actions telles que les pertes de paquets
CSCwf17814	ASA/FTD peut rechercher la source et recharger dans le nom de fil '19', échec de la somme de contrôle du blocage libre
CSCwf21106	ASA/FTD : Recherche de la source sur le nom du fil : snmp_master_callback_thread pendant les modifications de SNMP et d'interface
CSCwf22045	MYSQL, ou tout trafic TCP élevé, bloqué par snort3, avec snort-block comme raison d'abandon
CSCwf23564	Impossible d'établir BGP lors de l'utilisation de l'authentification MD5 sur le TUNNEL GRE et de FTD comme appareil d'intercommunication
CSCwf24124	Le processus SFDataCorrelator se bloque très fréquemment sur le FMC.
CSCwf24773	crashhandler exécuté avec le mode de test snort
CSCwf26939	FTD peut ne pas créer de règle NAT avec l'erreur suivante : « IPv4 dst real obj address range is huge »
CSCwf28488	Messages de journal incohérents vus lorsque l'indicateur est configuré et que la journalisation de la mémoire tampon est définie sur débogage
CSCwf30727	L'intégration de l'appareil de sécurité adaptable avec Cisco Umbrella ne fonctionne pas sans utilisation de validation ssl-server.
CSCwf31820	Les paquets ne sont pas transférés entre le VRF global vers le VRF de l'utilisateur et vice-versa
CSCwf33574	Les entrées de liste d'accès ASA ont le même hachage après la mise à niveau

ID du bogue	En-tête :
CSCwf34450	Plantage de Snort3 après le redémarrage de Snort si des applications personnalisées en double sont présentes
CSCwf35510	Segfault possible dans Snort3 lorsque appid tente de supprimer la table d'informations sur l'application
CSCwf51933	Échec de connexion par authentification extérieure pour le AAA-RADIUS après la mise à niveau
CSCwf54418	Réduire le temps nécessaire pour effacer les SA IKEv2 périmées formées après la détection en double
CSCwf60584	Surveillance de l'intégrité pour ne pas collecter les statistiques de routage pour le mode transparent FTD
CSCwf62885	Le mandataire à une seule branche FTDv derrière AWS GWLB abandonne en raison d'une somme de contrôle geneve-invalid-udp-checksum.
CSCwf71606	Listes de contrôle d'accès Cisco ASA et FTD non installées lors du rechargement
CSCwf73189	Cisco FTD abandonne le trafic GRE de WSA en raison d'une défaillance de la NAT
CSCwf76945	Les données des paquets sont toujours abandonnées après la mise à niveau
CSCwf85307	Les remplacements de politique IPS [Snort 3] ne fonctionnent pas sur les politiques de prévention des intrusions en chaîne
CSCwf88552	ASA/FTD : Recherche de la source et rechargement en raison de la réécriture de l'inspection NAT L7

Bogues résolus dans la version 7.2.4

Tableau mis à jour le : 25/02/2025

Tableau 36 : Bogues résolus dans la version 7.2.4

ID du bogue	En-tête :
CSCvo60131	Les enregistrements du journal d'audit ne s'affichent pas dans le bon ordre
CSCvq20057	Amélioration de la journalisation des sauvegardes de Secure Firewall (Firepower) et nouvelle tentative pour gzip lors de l'utilisation du stockage distant
CSCvq25866	Aperçu de la configuration Flex de \$SYS_FW_ENABLED_INSPECT_PROTOCOL_LIST déclenche une erreur
CSCvq70838	Recherche de la source dans la sortie de la commande tail-logs
CSCvs89229	Les règles incorrectes sont mises en surbrillance lors de la recherche dans les règles CA
CSCvu24703	FTD – Le déchargement de flux devrait pouvoir coexister avec la fonctionnalité de limitation de débit (QoS)

ID du bogue	En-tête :
CSCvv18009	L'exécution du suivi des paquets à l'aide de la sous-interface nameif entraîne une erreur
CSCvw90399	Problèmes de haute disponibilité de FMC avec trop de descripteurs de fichiers ouverts pour la connexion UDP sfipproxy
CSCvx24207	Objet FQDN contenant des adresses IPv4 et IPv6 Installer uniquement les entrées IPv6
CSCvx55978	Dégradation des performances dans l'API GetGroupDependency
CSCvx65032	Les flèches de déplacement de recherche d'ACL de FMC ne fonctionnent pas
CSCvx68173	Observations sur quelques instances de SNORT bloquées à 100 %
CSCvx71936	FXOS : Défaillance « The password encryption key has not been set. » affichée sur les appareils FPR1000 et FPR2100
CSCvx75441	Aperçu de la liste de fichiers : la suppression de deux listes ayant peu de contenus similaires lance la trace de pile sur FMC-UI
CSCvx86569	Règle de contrôle d'accès – Le commentaire disparaît si vous cliquez sur un autre onglet avant d'enregistrer le commentaire.
CSCvy26676	« Warning:Update failed/in-progress. » (Avertissement : échec de la mise à jour/en cours) Cosmétique après une mise à jour réussie
CSCvy38650	Impossible de télécharger le fichier capturé à partir de l'interface utilisateur des fichiers capturés par FMC
CSCvy45048	Paramètre de requête de sous-système ne filtre pas les enregistrements pour « auditrecords » restapi
CSCvz07004	SNORT2 : FTD effectue un serveur mandataire complet même lorsque la règle SSL comporte une action DND
CSCvz07712	Le déploiement échoue avec des erreurs internes - Impossible d'obtenir un nouvel ID
CSCvz19364	Aucun message syslog envoyé par FXOS quand duplex passe à « Half Duplex »
CSCvz34289	Dans certains cas, la transition vers un proxy allégé ne fonctionne pas pour les flux Ne pas déchiffrer
CSCvz36903	Recherche de la source et rechargement de l'appareil de sécurité adaptable lors de l'allocation d'un nouveau bloc pour le paquet Keepalive de la grappe
CSCvz40586	Erreur incorrecte lors de la création de deux profils RA-VPN avec différents serveurs SAML qui ont le même fournisseur d'identité
CSCvz41551	FP2100 : ASA/FTD avec statistiques de détection des menaces peut effectuer une recherche de la source et être rechargé dans le nom de fil « lina »
CSCvz42065	La politique IPS doit être importée lorsqu'elle est mentionnée dans la politique de contrôle d'accès
CSCvz71596	« Le nombre d'interfaces en mode actif et en mode veille n'est pas cohérent » devrait déclencher l'avertissement syslog
CSCvz77213	FTD : show ntp affiche le centre de données de gestion même si la synchronisation NTP est effectuée par FXOS

ID du bogue	En-tête :
CSCvz94841	Erreurs grammaticales dans le message d'erreur de non-concordance en mode de fonctionnement de basculement
CSCwa04262	Vulnérabilité de contournement des requêtes côté client SSL VPN du logiciel Cisco ASA via « / » URI
CSCwa16626	Syslog sur TLS acceptant un caractère générique au milieu du FQDN
CSCwa36535	L'unité de secours n'a pas pu rejoindre le basculement en raison d'une grande taille de configuration.
CSCwa59907	Recherche de la source observée par LINA sur le nom du fil « snmp_client_callback_thread »
CSCwa72481	Clé API corrompue pour FMC avec plusieurs interfaces
CSCwa72929	L'interrogation SNMPv3 peut échouer en utilisant les algorithmes de confidentialité AES192/AES256
CSCwa74063	Désactiver la solution de contournement d'installation des règles NLP après l'activation de l'accès de gestion dans NLP
CSCwa82850	Le basculement ASA ne détecte pas d'incompatibilité de contexte avant de déclarer que le nœud de jonction est « en veille »
CSCwa83133	FMC affichant « INVALID ID » (ID invalide) sous le gadget « Traffic by User » (trafic par utilisateur), mais erreur non vue dans les événements de connexion
CSCwa89116	Nettoyage du traitement des index de session dans IKEv2/SNMP/Session-mgr pour l'utilisation de MIB
CSCwa92822	Le client TLS dans le tunnel TLS sftunnel propose des courbes en mode CC qui ne sont pas autorisées par CC
CSCwa94440	Le processus syncd se termine en raison d'un GID non valide et d'un problème de synchronisation de la base de données
CSCwa96920	ASA/FTD peut rechercher la source et recharger dans le processus Lina
CSCwa97917	ISA3000 dans une boucle de démarrage après le cycle d'alimentation
CSCwb00749	Échec de la mise à niveau de FMC : échec de 114_DB_table_data_integrity_check.pl
CSCwb00871	ENH : réduire la latence dans log_handler_file pour réduire la surveillance en cas d'évolutivité ou de sollicitation
CSCwb02955	Modifier /800_post/1027_ldap_external_auth_fix.pl pour ne pas échouer la mise à niveau de FMC lorsque les objets sont corrompus
CSCwb03704	Les fils de chemin de données ASA/FTD peuvent se bloquer et générer la recherche de la source.
CSCwb04000	ASA/FTD : le bit DF est défini sur les paquets acheminés dans VTI
CSCwb04975	Recherche de la source FTD Snort3 dans daq-pdts lors du traitement du trafic basé sur le FQDN
CSCwb05291	Vulnérabilité d'exécution de code arbitraire côté client dans Cisco ASDM et le logiciel ASA

ID du bogue	En-tête :
CSCwb09606	FP2100 : La haute disponibilité ASA/FTD n'est pas résiliente à l'arrêt inattendu du processus LACP
CSCwb17362	Perte de la connexion SSH lors de la copie d'un fichier volumineux sur le périphérique, bien que le périphérique dispose de suffisamment d'espace.
CSCwb20206	FTD : Journaux et débogages pour la perte du trafic SSL/TLS en raison de NAP en mode de détection
CSCwb24306	Entrée de journal en double pour /mnt/disk0/log/asa_snmp.log
CSCwb31551	Lorsque le paquet entrant contient un en-tête SGT, FPR2100 ne peut pas distribuer correctement selon le tuple 5
CSCwb32107	FMC affiche des interfaces limitées dans la configuration de routage basée sur les politiques (sélection de l'interface de sortie)
CSCwb38961	Le démarrage après la mise à niveau a échoué en raison d'une clé en double de l'objet réseau
CSCwb42031	Vulnérabilité d'injection de code dans le logiciel Cisco FTD et FMC
CSCwb43433	Les performances des trames jumbo ont diminué jusqu'à -45 % sur la série Firepower 2100
CSCwb44048	Le taux d'événements sur le tableau de bord de surveillance de l'intégrité de FMC affiche des valeurs extrêmement élevées
CSCwb44848	Recherche de la source ASA/FTD et rechargement dans le processus Lina
CSCwb57213	FTD – Impossible de résoudre le DNS lorsque seule l'interface de diagnostic est utilisée pour les recherches DNS
CSCwb57524	Échec de la mise à niveau de FTD - Espace disque insuffisant en raison des anciens ensembles FXOS dans la partition distribuée
CSCwb58007	CVE-2022-28199 : évaluation pour FTDv et ASAv
CSCwb58554	Les sessions SSL reprises avec des billets non mis en mémoire cache peuvent échouer
CSCwb58817	FMC Déploiement des formes négatives et positives de la commande de mot de passe de BGP dans les déploiements
CSCwb60993	FDM doit bloquer le déploiement lorsqu'un objet de zone de sécurité n'est pas associé à une interface
CSCwb66382	ASAv – Le bloc 9344 n'est pas créé automatiquement après l'activation du bâti grand format, ce qui rompt le protocole OSPF MD5
CSCwb68993	FTD/FDM : Les connexions SSL aux sites utilisant des certificats RSA avec des clés de 3072 bits peuvent échouer
CSCwb78323	Veuillez mettre à jour diskmanager pour surveiller les fichiers cisco_uridb dans le dossier /ngfw/var/sf/cloud_download.
CSCwb80108	FP2100/FP1000 : Ports RJ45 intégrés ne s'activent pas de façon aléatoire après les événements de redémarrage du gestionnaire de ports
CSCwb84901	CIAM : Heimdal 1.0.1

ID du bogue	En-tête :
CSCwb86171	La rupture de FMCv HA dans AWS génère l'alerte « VTEP CONFIGURATION IS NOT SUPPORTED FOR CURRENT PERFORMANCE TIER » (La configuration VTEP n'est pas prise en charge pour le niveau de performances actuel).
CSCwb88406	Échec de la mise à niveau de FMC-HA en raison de la présence de ce fichier « update.status »
CSCwb88729	FTD – %FTD-3-99015 : port-manager : erreur : échec de lecture du bloc DOC, port X, st = X log
CSCwb89963	Recherche de la source ASA et rechargement dans le nom de fil : Datapath
CSCwb91598	La copie de la sauvegarde FMC vers un stockage distant échouera si FMC ne s'est jamais connecté par SSH/SCP à l'hôte distant
CSCwb92937	Erreur 403 : Interdite lors de l'expansion des objets de groupe d'affichage
CSCwb99375	Échec de la synchronisation de la configuration pour la commande « quit »
CSCwb99960	onPremFMC avec uniquement des périphériques gérés par CDO enregistrés, les pages d'événements de programmes malveillants affichent un avertissement de licence
CSCwc00115	Échec de l'enregistrement de FTD sur FMC local
CSCwc02488	ASA/FTD peut rechercher la source et recharger dans le nom de fil : 'None'
CSCwc03069	Les données internes de l'interface data0/0 sont activées/activées à partir de l'interface de ligne de commande, mais ascendantes/désactivées à partir de l'interrogation SNMP
CSCwc03332	FTD sur FP2100 peut prendre le relais en tant qu'unité active à haute disponibilité pendant le processus de redémarrage
CSCwc03393	Recherche de la source sur la ligne et taille du fichier principal supérieurs à 40 G avec échec de compression sur Cisco FTD
CSCwc03507	Aucun abandon de tampon sur les interfaces de données internes malgré peu de signes de saut de CPU
CSCwc04959	L'utilisation du disque est de 100 % sur les fichiers .dmp de FMC secondaires créés pour utiliser tout l'espace disque
CSCwc05375	AnyConnect SAML – L'invite de certificat client apparaît incorrectement dans le navigateur externe
CSCwc05434	FMC affiche « Fichier non stocké » après le téléchargement d'un fichier
CSCwc06833	Échec de déploiement avec ERROR Process Manager n'a pas pu vérifier l'ICDB de LSP
CSCwc07262	L'ASA de secours passe à la boucle de démarrage lors de la réplication de la configuration après la mise à niveau vers la version 9.16(3).
CSCwc08374	Adresse MAC du NIC de la carte réseau Azure ASA pour Gigeth 0/1 et 0/2 arrête de fonctionner après l'ajout d'interfaces
CSCwc08646	L'utilisateur sans mot de passe est invité à modifier le mot de passe lorsqu'il est connecté à partir du client SSH

ID du bogue	En-tête :
CSCwc08683	Voyant DEL de l'interface reste vert et clignote lorsque le câble SFP est débranchée sur le FPR1150
CSCwc10145	L'unité de grappe FTDv ne rejoint pas la grappe avec le message d'erreur « Échec de l'ouverture du connecteur d'écoute SSL NLP »
CSCwc10241	Déconnexion cérébrale de la haute disponibilité suite à une mise à niveau ou au redémarrage du périphérique
CSCwc10483	ASA/FTD – Recherche de la source dans le nom du fil : appAgent_subscribe_nd_thread
CSCwc11511	FTD : Défaillances de SNMP après la mise à niveau à la version 7.0.2
CSCwc11597	Recherches de la source ASA après la mise à niveau de SFR à la version 6.7.0.3
CSCwc13017	Recherche de la source et rechargement de FTD/ASA à l'adresse ../inspect/proxy.h:439
CSCwc18285	La commande Conn data-rate peut être activée ou désactivée en mode EXEC utilisateur non privilégié
CSCwc18524	Il manque des renseignements sur la tension ASA/FTD dans la commande « show environment »
CSCwc18668	La connexion échouée de l'utilisateur sur FMC n'enregistre pas l'entrée dans le journal d'audit lors de l'utilisation de l'authentification externe
CSCwc19124	Le déploiement de FMC ne démarre pas pour les périphériques de grappe
CSCwc20153	La configuration ICMP IPv6 est ajoutée et supprimée lors du déploiement de la politique
CSCwc20635	Cisco Firepower Threat Defense ICMPv6 avec vulnérabilité de déni de service Snort 2
CSCwc22170	Problème d'analyse SNORT perfstat / Hmdeamon ne démarre pas après un rapport de disque plein
CSCwc23113	La fonctionnalité LTP ne fonctionne pas sur l'ASA KP avec la version 9.18
CSCwc23844	Erreurs d'allocation d'UC et de mémoire de pile élevées ASAv malgré plus de 30 % de mémoire libre
CSCwc24582	Mettre à jour le diskmanager pour surveiller les répertoires de déploiement dans /ngfw/var/cisco/deploy/db
CSCwc24906	Recherche de la source et rechargement ASA/FTD sur l'ID de thread : 1637
CSCwc25683	JOBS_TABLE ne se purge pas si deployReports n'est pas disponible
CSCwc26406	FMC : Lenteur dans la page de gestion des périphériques
CSCwc26538	Avec des connexions d'accélération EFD évolutives, décélération à l'aide de la commande clear efd-throttle traceback lina
CSCwc26648	Recherche de la source et rechargement ASA/FTD dans le nom de fil Lina ou Datapath
CSCwc27236	Erreur JSON de surveillance de l'intégrité FMC
CSCwc27424	Impossible de supprimer la configuration FMC SAL sur site non utilisée
CSCwc27846	Recherche de la source et rechargement pendant la synchronisation à haute disponibilité après la mise à niveau et le rechargement.

ID du bogue	En-tête :
CSCwc28334	Vulnérabilité de fuite de clé privée Cisco ASA et FTD Software RSA
CSCwc28532	9344 Fuite de blocage en raison d'un trafic GRE fragmenté sur le traitement du flux interne de l'interface défini en ligne
CSCwc28684	Le MI se bloque et ne répond pas lorsque l'instance de conteneur FTD est rechargée
CSCwc28806	Recherche de la source et rechargement d'ASA sur le nom de processus Lina
CSCwc28928	ASA : Les débogages SLA ne s'affichent pas sur les sessions VTY
CSCwc31163	Échec de la mise à niveau de FPR1010 – Erreur lors de l'exécution du script 200_pre/100_get_snort_from_dc.pl
CSCwc31457	Processus ASA avec jeton en texte clair lorsqu'il n'est pas possible de le chiffrer
CSCwc32245	FMC : vérification de la validation pour empêcher l'expansion exponentielle des règles NAT
CSCwc32246	NAT64 traduit toutes les adresses IPv6 en 0.0.0.0/0 lorsque le sous-réseau d'objet 0.0.0.0 0.0.0.0 est utilisé
CSCwc33036	Journaux observés du côté du serveur syslog comme supérieur à la limite de messages configurée par/sec.
CSCwc33076	JOBS_TABLE n'est pas purgé en raison d'une violation de contrainte de clé étrangère dans policy_diff_main
CSCwc33323	FMC 7.0 – Réception de l'alerte « processus de surveillance de l'intégrité : aucun événement reçu pour le moment » pour plusieurs périphériques
CSCwc34818	L'enregistrement du périphérique est annulé lorsque l'API REST appelle le script.
CSCwc35181	Le modèle OSPF ajoute « default-information-originate » à la zone <area-id> nssa en cliquant sur OK.
CSCwc35583	Fuite des descripteurs de fichier Snort avec chaque fichier u2 créé
CSCwc35969	Impossible d'ajouter l'adresse IP de l'événement aux listes globales (blocage ou non-blocage) si une adresse IP similaire est déjà dans la liste
CSCwc36905	Recherche de la source et rechargement de l'appareil de sécurité adaptable en raison de « mémoire du tas corrompue au niveau de slib_malloc.c »
CSCwc37061	SNMP : FMC ne répond pas à l'OID 1.3.6.1.2.1.25.3.3.1.2
CSCwc37256	Accès SSL AnyConnect bloqué après la mise à niveau
CSCwc37695	En plus de l'injection de commande shell c_rehash identifiée dans CVE-2022-1292
CSCwc38500	FMC : L'objet d'ACL étendu doit prendre en charge les protocoles mixtes sur différentes entrées
CSCwc38567	ASA/FTD peut effectuer une recherche de la source et se recharger pendant l'exécution du code SCH
CSCwc40352	Lina Netflow envoie des événements autorisés à Stealthwatch, mais ils sont ensuite bloqués par Snort

ID du bogue	En-tête :
CSCwc40381	ASA : Problème d'authentification du trafic HTTPS avec le mandataire de bout en bout activé
CSCwc41180	AWS ASAv Clustering : enable cluster breaking ssh session (activer la session ssh de rupture de grappe)
CSCwc41592	Faux-positifs pour Ultrasurf
CSCwc41728	FMC – Impossible de modifier l'ACL standard avec une erreur concernant « Uniquement les objets hôtes autorisés »
CSCwc42174	CIAM : Mariadb – plusieurs versions CVE-2022-32081
CSCwc42176	CIAM : Mariadb – plusieurs versions CVE-2022-32082
CSCwc42179	CIAM : Mariadb – plusieurs versions CVE-2022-32084
CSCwc42186	CIAM : Mariadb – plusieurs versions CVE-2022-32089
CSCwc42561	Le déploiement de la liste de pages prend de 1,5 à 2 minutes avec l'appareil 462 HA
CSCwc43807	FTD est inutilisable après le redémarrage si Manager est supprimé et si FIPS est activé
CSCwc44289	FTD– Recherche de la source et rechargement lors des traductions NAT IPv4 <=> IPv6
CSCwc44608	Le déploiement sélectif d'IPS peut entraîner une panne en raison de fichiers de configuration FTD mal écrits
CSCwc45108	ASA/FTD : Inspection GTP à l'origine d'une fuite de blocs de taille 9 344
CSCwc45397	ASA HA – Restaurer dans le serveur principal et ne pas supprimer la nouvelle configuration d'interface effectuée après la sauvegarde
CSCwc45575	Recherche de la source ASA/FTD et rechargement lors de l'utilisation de SSH à l'aide d'un nom d'utilisateur avec mot de passe nopasssword
CSCwc45759	Les journaux NTP remplaceront éventuellement tous les journaux de noyau Oxeon utiles
CSCwc46847	Partition FXOS opt_cisco_platform_logs sur FP1K/FPR2K peut être pleine en raison du fichier ucssh_*.log
CSCwc47586	Échec de la mise à niveau de vFMC 7.0.4-36> 7.3.0-1553 : erreur lors de l'exécution du script 200_pre/007_check_sru_install.sh
CSCwc48375	SA IPSEC entrante bloquée inactive – de nombreux SPI entrants pour un SPI sortant dans « show crypto ipsec sa » (afficher crypto ipsec sa)
CSCwc48853	Le goulot d'étranglement de l'événement de découverte SFDataCorrelator peut entraîner un retard et un arriéré de l'événement de connexion.
CSCwc49095	Recherche de la source et rechargement pour la plateforme ASA/FTD 2100 lorsque les fragments sont fusionnés et envoyés à PDTs
CSCwc49364	Processus mojo_server redémarrant inutilement pendant la rotation du journal
CSCwc49369	Lors de la recherche d'une règle IPv6 dans la politique de contrôle d'accès, aucun résultat ne s'affiche

ID du bogue	En-tête :
CSCwc49936	Intégration FMC 7.2.0 7.3.0 > La page Sources d'identité ne se charge pas et continue de tourner
CSCwc49942	Recharger mercury lorsque le fichier userappid.conf est modifié sur FMC et que le déploiement est émis
CSCwc49952	Le déploiement sélectif permet l'interface avec les politiques interdépendantes SRU en raison de l'expiration de l'API FMC
CSCwc50098	show ssl-policy-config n'affiche pas la politique lorsque les pays sont utilisés dans le réseau source/destination
CSCwc50519	Une journalisation excessive à partir de HM_pm peut entraîner le redémarrage du processus syslog-ng
CSCwc50846	Échec de la mise à niveau de FTD – Vérification de l'état de préparation réussie, mais état de l'état de préparation jamais affiché
CSCwc50887	FTD – Recherche de la source et rechargement sur NAT IPv4<> IPv6 pour le flux UDP redirigé sur le lien CCL
CSCwc50891	Balisage MPLS supprimé par FTD
CSCwc51326	Plateforme Firepower basée sur FXOS affichant des abandons « sans tampon » malgré les valeurs élevées des filigranes de l'anneau RX
CSCwc52351	Déconnexion cérébrale de grappe ASA/FTD en raison d'une NAT avec « tout » et d'une adresse IP globale/plage correspondant à l'adresse IP de diffusion
CSCwc52357	Échec de chargement de la page EStreamer dans ASDM
CSCwc53280	L'analyseur ASA accepte une instruction de réseau incomplète sous le processus OSPF et est présente dans l'exécution de l'affichage
CSCwc54217	le journal système associé au basculement n'est pas sorti dans FPR2140
CSCwc54901	Les tâches planifiées peuvent ne pas s'exécuter sur FMC actif en mode haute disponibilité après le basculement ou la résolution de déconnexion cérébrale
CSCwc54984	IKEv2 rekey – Réponse du SPI non valide pour le nouveau SPI reçu immédiatement après la réponse de Create_Child_SA
CSCwc56003	Échec du déclenchement de la sauvegarde FTD avec l'option de stockage à distance activée ainsi que de la récupération dans FMC
CSCwc56048	Le nom d'utilisateur AD avec un espace de fin entraîne l'échec du téléchargement des utilisateurs/groupes
CSCwc56952	Possibilité de voir les journaux de débogage SLA sur les sessions de console et de VTY, même si nous l'activons uniquement sur la session VTY.
CSCwc57088	Limiter le nombre de tâches de déploiement dans l'historique de déploiement à 50 par défaut pour éviter la lenteur
CSCwc57575	FMC : Les sauvegardes planifiées fonctionnent bien, mais alertes par courriel de FMC l'indiquant comme échec.

ID du bogue	En-tête :
CSCwc60037	L'appareil de sécurité adaptable ne parvient pas à se renouveler avec l'ERREUR IPSEC : n'a pas pu être alloué un contexte matériel sortant
CSCwc60907	Mise à jour de l'identifiant de validation WR6, WR8, LTS18 et LTS21 dans la couche CCM (séqu. 35)
CSCwc60943	FMC : L'enregistrement peut échouer avec une erreur de nom en double après la modification d'un nom d'appareil au moyen de l'interface utilisateur
CSCwc61132	KP-2130 – Plantage observé avec PPK configuré
CSCwc61912	ASA/FTD OSPFv3 ne génère pas de messages LSA de type 8 pour IPv6
CSCwc62144	FMC n'utilise pas de serveur mandataire avec authentification lors de l'accès aux services en nuage AMP
CSCwc62384	Vulnérabilités sur le portail Cisco FTD sur le port TCP 885
CSCwc63273	La requête de délai d'expiration de l'hôte SFDataCorrelator peut bloquer le traitement des événements et entraîner un redémarrage avec blocage
CSCwc64333	Délai d'expiration de l'interface graphique du FMC et problèmes de chargement de la page http en raison d'un nombre excessif de connexions http
CSCwc64923	ASA/FTD peut rechercher la source et recharger dans le nom de fil « lina » ip routage ndbshr
CSCwc66671	Rapport PDF de FMC généré en vide/0 octet à l'aide de l'interface utilisateur
CSCwc66757	ASA/FTD peut rechercher la source et recharger dans le nom de fil « lina »
CSCwc67031	Le concentrateur vti avec des connexions de trous d'épingle compatibles avec le protocole NAT-T boucle et entraîne des interruptions d'activité du SNORT
CSCwc67687	Le basculement d'ASA HA déclenche l'échec du redémarrage du serveur HTTP et la panne ASDM
CSCwc67886	ASA/FTD peut effectuer une recherche de source et rechargement dans le nom de fil « lina_inotify_file_monitor_thread »
CSCwc68543	incompatibilité dans la configuration poussée à partir de FMC et en cours d'exécution sur FTD
CSCwc68656	CLI ASA pour TCP Nombre maximal de segments non traités
CSCwc69583	Le canal de port configuré à partir des interruptions FDM « utilise les interfaces de données comme passerelle » pour l'interface de gestion
CSCwc69992	Les licences essentielles ne sont pas attribuées au périphérique et les licences de modification ne fonctionnent pas non plus
CSCwc70962	Le mode « Write Standby » (En attente d'écriture) de FTD/ASA active les chiffrements ECDSA, ce qui entraîne l'échec d'établissement de liaison SSLv3 CA
CSCwc72155	Recherche de la source ASA/FTD et rechargement sur la fonction « snp_cluster_trans_allocb »
CSCwc72284	La comptabilité TACACS comprend une adresse IPv6 incorrecte du client

ID du bogue	En-tête :
CSCwc73224	La configuration de l'appel local sur le périphérique de secours est perdue après le rechargement.
CSCwc74099	Le fuseau horaire de l'appareil de sécurité adaptable FPR2140 revient à l'heure UTC après le redémarrage ou le rechargement du périphérique
CSCwc74103	ASA/FTD peut rechercher la source et rechargement dans le nom de fil « DATAPATH-11-32591 »
CSCwc74378	L'interface utilisateur de FMC ne devrait pas autoriser la désactivation simultanée des canaux de gestion de l'interface et d'événements de FMC.
CSCwc74841	Le flux RSS de FMC est interrompu, car FeedBurner n'est plus actif - « Impossible d'analyser le flux »
CSCwc74858	FTD - Recherche de la source dans le nom du fil : DATAPATH
CSCwc75061	FMC permet d'accéder à l'interpréteur de commandes pour le nom d'utilisateur avec « . », mais l'authentification extérieure échouera
CSCwc75082	25G-SR devrait prendre la valeur RS-FEC (IEEE CL108) par défaut plutôt que FC-FEC
CSCwc76195	Les interfaces Fail-To-Wire oscillent par intermittence en raison de l'expiration du délai de surveillance dans la plateforme Firepower 2100
CSCwc76700	Vulnérabilité de script intersite stockée dans le logiciel Cisco Firepower Management Center
CSCwc76913	cdFMC : Le déploiement de la politique échoue après la mise à niveau de cdFMC
CSCwc77519	FPR1000 ASA/FTD : le serveur principal joue un rôle actif après le rechargement
CSCwc77680	FTD peut rechercher la source et recharger dans le nom de fil « DATAPATH-0-4948 »
CSCwc77892	Erreurs CGroups dans le journal système ASA après le démarrage
CSCwc78296	La base de données peut ne pas s'arrêter ou ne pas démarrer correctement pendant la mise à niveau
CSCwc79366	Pendant le déploiement, l'appareil est bloqué dans le traitement de la demande de configuration.
CSCwc79682	FMC 7.1+ permet le déploiement d'ECMP FlexConfig
CSCwc80234	Différence de configuration « inspect snmp » entre actif et veille
CSCwc80357	Dégradation [Deploy Performance] dans la page de déploiement sur FMC
CSCwc81184	Recherche de la source ASA/FTD et rechargement causés par une défaillance du processus SNMP
CSCwc81219	Les événements d'intrusion cessent de s'afficher dans FMC par intermittence lors de l'utilisation de SNORT3
CSCwc81727	Le domaine par défaut dans les objets de politique de groupe VPN ne peut pas être supprimé.
CSCwc81945	Le trafic sur l'unité de données est abandonné avec « LU allocate xlate failed » sur la grappe GCP avec l'interface NAT

ID du bogue	En-tête :
CSCwc81960	Impossible de configurer « match ip address » sous la carte de routage lors de l'utilisation d'un groupe d'objets dans la liste d'accès
CSCwc82124	Règles de NAT ASA ne fonctionnent pas comme prévu après une mise à niveau à la version 9.18.2
CSCwc82188	Recherche de la source FTD et rechargement lors de l'application de commandes longues à partir de l'interface utilisateur de FMC ou de CLISH
CSCwc83037	Mise à jour de l'identifiant de validation WR6, WR8, LTS18 et LTS21 dans la couche CCM (séqu. 36)
CSCwc83346	Recherche de la source et rechargement ASA/FTD dans le Threadname : Daemon IKE
CSCwc86197	Vulnérabilités dans Mariadb – Plusieurs versions CVE-2022-32091
CSCwc86330	Vulnérabilités dans spring-framework – Plusieurs versions CVE-2022-22970
CSCwc86391	Sur les réseaux lents avec quelques pertes de paquets, sftunnel peut marquer les connexions comme STALE
CSCwc87387	Les demandes DNS valides sont abandonnées par l'inspection DNS de Lina lorsque le DNS Umbrella est configuré
CSCwc87441	Pour les processus système, limiter les CPU utilisées au nombre de CPU système
CSCwc87963	ASAv : « Impossible de récupérer les informations de licence. Veuillez réessayer plus tard »
CSCwc88108	Politique de préfiltre : temps de réponse long dans le menu de port disponible, la recherche de réseau de préfiltre prend beaucoup de temps
CSCwc88425	FMC ne peut télécharger que les 10 000 premiers groupes d'utilisateurs interdomaine
CSCwc88629	La suppression d'un groupe pendant le téléchargement de domaine peut entraîner une carte utilisateur_to_group incohérente sur FTD
CSCwc88897	Recherche de la source et rechargement d'ASA en raison d'un pointeur nul dans Umbrella après la modification de la politique d'inspection DNS
CSCwc89661	FTD manque les données de diagnostic nécessaires pour enquêter sur l'erreur « Communication avec NPU perdu »
CSCwc89796	ASA/FTD peut effectuer une recherche de la source et se recharger dans la détection de l'homologue « appagent_async_client_receive_thread » du nom de fil
CSCwc89924	OID SNMP FXOS ASA/FTD pour interroger les compteurs de l'interface « sans tampon » de données internes
CSCwc90091	L'ASA 9.12(4)47 avec des statistiques d'utilisateurs affectera la visibilité « policy-server xxxx global ».
CSCwc91451	noyau de concentrateur dvti à l'adresse ctm_sw_ipsec_nettoyage_fragments+394
CSCwc92761	7.3 – Flux de messages par utilisation d'une valeur non initialisée \$unix_time dans gt numérique
CSCwc93166	L'utilisation du mode veille d'écriture dans un contexte d'utilisateur laissera l'état de licence de pare-feu secondaire dans un état non valide

ID du bogue	En-tête :
CSCwc93964	ASA utilisant des retours en arrière WebVPN dans le fil Unicorn lors du suivi de la mémoire
CSCwc94085	Impossible d'établir DTLSv1.2 avec FIPS activé après la mise à niveau à partir de la version 6.6.5.
CSCwc94267	Unité de grappe désactivée enregistrée en tant qu'unité autonome dans FMC et échec du déploiement ultérieur
CSCwc94466	Vulnérabilité du déni de service SSL/TLS de Cisco ASA/FTD Firepower 2100
CSCwc94501	Fuite de mémoire ASA/FTD et recherche de la source en raison des réinitialisations ctm_n5
CSCwc94547	Recherche de la source Lina et rechargement lors de l'émission « debug menu FXOS_parser 4 »
CSCwc94670	Fuite de mémoire dans svc_sam_statsAG dans TPK
CSCwc95290	La règle ESP manquante dans vpn-context peut entraîner une perte du trafic IPSec
CSCwc96016	Prise en charge des portails captifs dans plusieurs domaines
CSCwc96136	CCM, séq. 38 – WR8, LTS18, LTS21
CSCwc96726	R2130 utilise le site distant/la succursale du système d'exploitation Wave CIS_LTS21_R2130 pour la version 7.3.0 bêta 2.
CSCwc96780	L'exclusion de l'intégrité spécifique au module FMC désactive toutes les vérifications de l'intégrité
CSCwc96805	traceback and reload due to tcp intercept stat in thread unicorn (recherche de la source et rechargement en raison de la stat d'interception TCP dans le fil unicorn)
CSCwc97260	Redémarrage continu du processus ngfwManager en raison d'un enregistrement incomplet du périphérique FMC à haute disponibilité
CSCwc98997	FMC – Déploiement bloqué lorsque la route ECMP est configurée via la même interface
CSCwc99242	Port SFP membre du canal ISA 3000 LACP suspendu après le rechargement
CSCwd00386	ASA/FTD peut effectuer une recherche de source et se recharger lors de l'effacement de la configuration en raison de « snp_clear_acl_log_flow_all »
CSCwd00583	La chaîne SNMP « Confirmer la chaîne de communauté » n'est pas remplie automatiquement après la mise à niveau de FMC
CSCwd00778	La sortie ifAdminStatus est anormale via l'interrogation snmp
CSCwd01032	ASA/FTD peut rechercher la source et recharger lorsque RAVPN avec SAML est configuré
CSCwd02864	logging/syslog is impacted by SNMP traps and logging history (la journalisation/syslog est affectée par les dérouterments SNMP et l'historique de journalisation)
CSCwd02925	Vulnérabilité de l'injection de commande du logiciel Cisco Firepower Management Center
CSCwd03104	L'état de la grappe n'est pas mis à jour dans l'ensemble de la grappe GCP à 16 nœuds

ID du bogue	En-tête :
CSCwd03113	La sauvegarde locale du FMC échoue en raison de « Update Task : échec de la vérification de l'intégrité de la base de données » – Problème de serveur Syslog
CSCwd03793	Recherche de la source et rechargement de FTD
CSCwd03810	La page de connexion personnalisée ASA ne fonctionne pas par webvpn après une mise à niveau
CSCwd04135	Snort3 abandonne des paquets de manière inattendue après 4 Mo lors de l'utilisation de l'inspection de fichier avec le mode de détection NAP
CSCwd04210	ASA : Sessions ASDM bloquées dans CLOSE_WAIT, ce qui entraîne un manque de MGMT
CSCwd05443	Config-dispatcher doit échouer le déploiement immédiatement lorsque le téléchargement échoue, au lieu d'échouer ultérieurement
CSCwd05756	Recherche de la source FTD sur Lina en raison d'un composant du journal système.
CSCwd05772	Vulnérabilité d'écriture de fichier arbitraire du logiciel Cisco FXOS
CSCwd05814	L'écriture PDTS à partir de Daq peut échouer lorsque la mémoire tampon PDTS est pleine, ce qui entraîne éventuellement l'épuisement du blocage
CSCwd06005	Recherche de la source et rechargement ASA/FTD pendant la sortie du nœud
CSCwd07059	Plusieurs plantages de Snort3 après la mise à niveau de FTD de la version 7.2.0 à la version 7.2.0.1
CSCwd07278	Vérification de la validation de la correspondance ASA/FTD lorsque l'unité rejoint la grappe, lorsque TCM est désactivé
CSCwd07413	FMC - Modification des interfaces membres sur le canal de port bloquée dans la fenêtre de mise à jour de l'interface
CSCwd08402	L'URI HTTP est parfois manquant dans la vue des incidents d'intrusion
CSCwd08430	Créer une option de configuration de résilience pour SFTunnel afin de prendre en charge la connectivité à haute disponibilité et FTD
CSCwd09093	La page de politique de règles d'accès prend plus de temps à se charger
CSCwd09231	Vulnérabilité de script intersite du logiciel Cisco Firepower Management Center
CSCwd09341	Plusieurs fichiers de journalisation n'ont aucun octet en raison d'un échec de journalisation
CSCwd09870	Échec intermittent de AnyConnect SAML à l'aide d'un navigateur externe et d'un DNS tourniquet
CSCwd09967	Le déploiement échoue avec stacktrace : type non valide (LocalIdentitySource)
CSCwd10497	Règles de capteur FTD manquantes dans le fichier ngfw.rules après l'exécution d'une restauration de sauvegarde de capteur
CSCwd10880	Alertes d'intégrité critiques « user configuration(FSM.sam.dme.AaaUserEpUpdateUserEp) » sur FPR 1100/2100/3100

ID du bogue	En-tête :
CSCwd11005	Le fichier fqdns_old.conf manquant entraîne l'échec de la synchronisation de l'application FTD à haute disponibilité
CSCwd11165	L'option « Move » (déplacer) est grisée sur l'option de sauvegarde-restauration dans FMC.
CSCwd11303	L'ASA peut générer une recherche de la source dans le processus IKEv2 et un rechargement
CSCwd11855	ASA/FTD peut générer une recherche de la source et recharger dans le nom de thread « ikev2_fo_event »
CSCwd12334	Le déploiement échoue avec l'erreur de configuration -- proxy paired
CSCwd13083	FMC Impossible de lancer le déploiement en raison d'une validation incorrecte de la licence de menace
CSCwd13917	during download from file event on FMC, high CPU use on FMC for 20 minutes before download fails (pendant le téléchargement à partir d'un événement de fichier sur FMC, utilisation élevée du processeur sur FMC pendant 20 minutes avant l'échec du téléchargement)
CSCwd14688	Échec de la mise à niveau de FTD en raison de la génération ou de la suppression rapide des fichiers Syslog
CSCwd14732	FTD Impossible de se lier au port 8305 après la modification de l'IP de gestion
CSCwd14972	Recherche de la source et rechargement ASA/FTD dans le nom du fil : pix_flash_config_thread
CSCwd16017	Lenteur de modification d'objet lorsqu'il est associé à des règles de NAT
CSCwd16294	L'inspection GTP abandonne les paquets pour la longueur d'en-tête IE facultative étant trop courte
CSCwd16517	Abandons GTP pas toujours enregistrés dans la mémoire tampon et le journal système
CSCwd16689	Recherche de la source ASA/FTD en raison d'une corruption de données de blocage
CSCwd16712	Échec de la vérification de la mise à niveau de la disponibilité du périphérique – Problème de synchronisation de sftunnel en raison d'un changement de temps
CSCwd16902	Les événements de fichier affichent l'action comme « Blocage de programmes malveillants » pour les fichiers avec une disposition correcte de l'inconnu
CSCwd16906	ASA/FTD peut effectuer une recherche de source et recharger dans le nom de fil « lina » après le déploiement de la politique
CSCwd17037	L'action SFDataCorrelator RNA-Stop ne doit pas bloquer lorsque les opérations de base de données sont suspendues
CSCwd17856	L'appareil de sécurité adaptable recherche la source/le recharge avec le message : snmp_ma_kill_restart : vf est NULL
CSCwd17940	La haute disponibilité n'a pas basculé en raison de mises à jour d'état incorrectes de NDClient

ID du bogue	En-tête :
CSCwd18744	FTD FPR1K ne parvient pas à former la haute disponibilité en raison de la raison « autre unité a un ensemble différent d'index hwidb »
CSCwd19053	ASA/FTD peut effectuer une recherche de la source avec un grand nombre d'objets réseau déployés à l'aide de la liste de distribution
CSCwd20627	ASA/FTD : Échec du déploiement de la configuration de la NAT
CSCwd20900	Les pages de réponse au blocage HTTP et de réponse au blocage interactif ne sont pas affichées par Snort3
CSCwd22349	ASA : impossible de connecter l'authentification basée sur le certificat AnyConnect avec le « certificat d'authentification périodique » activé
CSCwd22413	ASA/FTD : Recherche de la source et rechargement dans le nom du fil : EIGRP-IPv4
CSCwd22907	UC élevée ASA/FTD dans le fil de notification SNMP
CSCwd23188	ASA/FTD peut rechercher la source et recharger dans le nom de fil « lina »
CSCwd23913	FTD dans la haute disponibilité recherche de la source plusieurs fois après l'ajout d'un voisin de BGP avec liste de préfixes.
CSCwd24072	L'emplacement de stockage rsc_5_min.log doit être déplacé vers une autre partition
CSCwd24289	Numéro de série du certificat ne s'affiche pas correctement dans les journaux de débogage et syslog de PCA
CSCwd24639	Fonctionnel : la mise à niveau de correctif FMCv échoue
CSCwd25201	Interruptions SNMP ASA/FTD mises en file d'attente lorsqu'aucun serveur d'interruption SNMP n'est configuré
CSCwd25256	La validation transactionnelle ASA/FTD peut entraîner des règles non concordantes et une perte de trafic
CSCwd26466	Alerte d'événements de vidange fréquents incorrecte
CSCwd26867	L'appareil ne doit pas passer à l'état actif une fois le redémarrage déclenché
CSCwd28037	Aucun nameif pendant le trafic entraîne la recherche de la source du périphérique, le cœur lina est généré.
CSCwd28236	Unité de secours utilisant des adresses IP actives et en veille, ce qui entraîne des problèmes d'adresses IP en double en raison de la traduction d'adresses IP « any »
CSCwd29835	Échec de rotation du journal pour cycler les fichiers, ce qui entraîne une taille de fichier volumineuse
CSCwd30774	FMC HA : les fichiers dans tmp/Sync sont laissés en secondaire lorsque la tâche de synchronisation échoue
CSCwd30856	L'utilisateur sans filtre vpn peut obtenir un accès supplémentaire lorsque le remplacement par utilisateur est défini
CSCwd30977	FMC a supprimé certaines règles d'accès en raison d'un chiffre incorrect généré lors du déploiement de la politique.

ID du bogue	En-tête :
CSCwd31181	Recherche de la source Lina et redémarrage – le canal parent du VPN (SAL) a un canal sous-jacent non valide
CSCwd31960	L'accès à la gestion sur le VPN ne fonctionne pas lorsque la NAT personnalisée est configurée
CSCwd32892	cac.conf perdu après la mise à niveau à la version 7.2.1 pour l'authentification des cartes à puce de FMC
CSCwd33054	Le relais DHCP effectue une boucle avec retour du paquet d'offre DHCP, ce qui entraîne l'échec de dhcprelay sur le FTD/ASA
CSCwd33479	Paquets d'ID de session SMB en double ce qui provoque le plantage de snort3
CSCwd33721	Le processus ADI peut devenir instable lors du téléchargement d'un grand nombre d'utilisateurs
CSCwd33811	L'enregistrement de la grappe a échoué, car Data_node ne rejoint pas la grappe
CSCwd34662	Mise à jour de l'identifiant de validation LTS18 et LTS21 dans la couche CCM (séqu. 39)
CSCwd35726	Vulnérabilité d'écriture de fichier arbitraire du logiciel Cisco FXOS
CSCwd36246	Le filtrage des tâches dans la page d'historique de déploiement applique les critères uniquement aux tâches Top50
CSCwd37135	Recherche de la source ASA/FTD et rechargement sur le nom du fil fover_fail_check
CSCwd37238	Les connexions TLS au serveur Exchange 2007 peuvent échouer
CSCwd37718	Prévention des défaillances de sonde de pulsation de grappe dans la plateforme virtuelle
CSCwd38526	FMC peut autoriser le déploiement de NAP en mode test avec la politique de déchiffrement
CSCwd38774	ASA : Recherche de la source et rechargement en raison de la fermeture de la session webvpn sans client
CSCwd38775	ASA/FTD peut rechercher et recharger dans le processus Lina
CSCwd38805	Syslog 106016 n'est pas limité par défaut
CSCwd39039	FMC – Message d'erreur « La réponse du serveur n'a pas été comprise. Communiquer avec le service de soutien à la clientèle » sur l'interface utilisateur.
CSCwd39468	Recherche de la source ASA/FTD et rechargement lors de la configuration des captures ISAKMP sur le périphérique
CSCwd39710	Retard SFDataCorrelator dans le traitement des événements lorsque le taux d'incidents d'intrusion est élevé
CSCwd40141	L'affichage de l'interface graphique de Firepower Management Center pour les règles de prévention des intrusions locales Snort2 est manquant
CSCwd40260	Amélioration de la convivialité – Impossible d'analyser la charge utile qui est abandonnée en silencieux par ASA/FTD
CSCwd40955	Délai de validation très long pendant le déploiement de la politique en raison d'un objet réseau volumineux dans la politique SSL

ID du bogue	En-tête :
CSCwd41083	Recherche de la source et rechargement de l'appareil de sécurité adaptable en raison de l'inspection DNS
CSCwd41224	Interface utilisateur Web à haute disponibilité du FMC ne reçoit pas le niveau de variable FTDv affecté à FTDv - Variable
CSCwd41466	Les utilisateurs téléchargés à nouveau à partir d'une forêt avec des domaines de confiance peuvent ne pas être résolus ou non synchronisés
CSCwd41553	Les paquets de registre PIM ne sont pas envoyés au point de rendez-vous (RP) en raison de l'état de panne de l'interface de tunnel PIM
CSCwd41806	deployment failed with OOM (out of memory) for policy_apply.pl process (échec du déploiement avec OOM (mémoire saturée) pour le processus policy_apply.pl)
CSCwd42620	Le déploiement d'objets avec des valeurs échappées dans la description peut entraîner l'échec de tous les déploiements futurs.
CSCwd43666	Analyse de la raison pour laquelle il n'y a pas de logrotate pour /opt/cisco/config/var/log/ASAconsole.log
CSCwd44326	Échec de la modification de la NAT de l'objet
CSCwd46741	La rotation du journal FXOS ne parvient pas à recycler les fichiers, ce qui entraîne une taille de fichier volumineuse
CSCwd46780	ASA/FTD : Recherche de la source et rechargement dans le nom du fil : appAgent_reply_processor_thread
CSCwd47340	Fuite de mémoire dans le processus svc_sam_envAG
CSCwd47424	Le nom de l'appareil s'affiche toujours comme « firepower » dans la vue des événements CDO
CSCwd47442	Erreur de mise à niveau 800_post/1027_ldap_external_auth_fix.pl – référence pour un objet d'authentification manquant
CSCwd47481	Mise à jour de l'identifiant de validation WR6, WR8, LTS18 et LTS21 dans la couche CCM (séqu. 40)
CSCwd48633	ASA – recherche de la source et rechargement lorsque le portail Webvpn est utilisé
CSCwd48776	L'interface du canal de port est survenue après le déploiement
CSCwd49636	Interface utilisateur de FMC affichant désactivé/ hors ligne pour plusieurs périphériques, car les événements d'intégrité ne sont pas traités
CSCwd49685	MEMCAP SSL manquant entraîne l'échec du déploiement en raison du délai d'attente des moteurs de détection SNORT
CSCwd49758	Échec de prédéploiement observé dans FMC en raison d'un nombre très élevé de politiques
CSCwd50131	Les mises à niveau ne nettoient pas les fichiers mysql ce qui entraîne une alerte pour « Utilisation élevée du disque non géré sur /ngfw »
CSCwd50218	La restauration de l'appareil de sécurité adaptable n'applique pas la configuration VLAN

ID du bogue	En-tête :
CSCwd51757	Impossible d'obtenir les résultats de l'interrogation en utilisant snmp GET pour les OID\2019s de débit de connexion
CSCwd51964	Ajout de la validation dans l'API du détecteur lua pour vérifier les modèles vides pour les applications de service
CSCwd52448	La fuite de route de l'hôte local ayant un masque /32 peut entraîner un plantage
CSCwd52995	FMC n'ouvre pas la fenêtre d'aperçu du déploiement
CSCwd53135	ASA/FTD : Journal système de recherche de groupe d'objets pour les flux dépassant le seuil
CSCwd53340	La file d'attente RX FTD PDTS LINA peut se bloquer lorsque le Snort envoie des messages d'une taille de 4 085 à 4 096 octets
CSCwd53448	FPR3100 : Voyants DEL du module de réseau 4 x 40 ne clignent pas lorsqu'il y a du trafic
CSCwd53635	AWS : Échec du déchiffrement SSL avec l'interface de tunnel Geneve
CSCwd53863	La migration des données de Sybase vers MariaDB prend plus de temps en raison de la grande taille des données de POLICY_SNAPSHOT
CSCwd54360	FP2100 : Modifications du côté de FXOS pour la haute disponibilité ne sont pas résilientes au problème inattendu d'arrêt du processus LACP
CSCwd54439	FMC envoie un message d'erreur non pertinent pour l'échec de conversion des règles Snort2 en Snort3
CSCwd55673	Corrections nécessaires dans le correctif de plantage de la surveillance de log_handler_file
CSCwd55853	FDM : Échec de déploiement avec erreur de chevauchement de groupe local après la mise à niveau
CSCwd56254	La génération « show tech-support » n'inclut pas « show inventory » lorsqu'elle est exécutée sur FTD
CSCwd56296	Recherche de la source et rechargement Lina dans le nom de fil « IP Init Thread »
CSCwd56431	Désactiver les vérifications dans les versions de production de FTD
CSCwd56654	Défaillances de plateforme liées à l'interface de gestion sur FXOS
CSCwd56774	Raison de l'abandon incorrecte dans « show asp drop »
CSCwd56834	[IMS_7_3_0/7_2_0] Lina a planté sur la grappe de nœuds VMware 2 lors de l'envoi du trafic GRE
CSCwd56995	Accès sans client au contenu Web à l'aide de application/octet-stream vs text/plain
CSCwd57698	État d'urgence récursif sous lina_duart_write
CSCwd57784	L'archive de configuration doit être créée si la méthode Rest-GET a échoué sur le périphérique
CSCwd58188	État de la paire en ligne n'a pas pu passer du mode de contournement matériel au mode veille

ID du bogue	En-tête :
CSCwd58337	Allouer plus de mémoire de groupe c pour le sous-groupe de déploiement des politiques
CSCwd58417	La synchronisation périodique de la haute disponibilité échoue en raison d'un fichier cfg manquant
CSCwd58430	Parfois, l'enregistrement de la politique CA prend plus de temps, peut aller jusqu'à 10 minutes ou plus
CSCwd58528	Épuisement de la mémoire lors de l'exécution du profil de trafic EMIX sur le nœud actif à haute disponibilité de QP
CSCwd59736	ASA/FTD : Recherche de la source et rechargement en raison de la configuration du groupe SNMP pendant la mise à niveau
CSCwd61016	ASA : Le périphérique en veille peut être bloqué dans l'état « Sync Config » au redémarrage, lorsqu'EEM est configuré
CSCwd61082	Interface utilisateur du FMC affichant des données inexactes dans la page de supervision du VPN S2S
CSCwd61410	mdbtrace.log peut remplir le stockage sur FMC
CSCwd62025	FTDv : Échec du déploiement de la politique en raison du paramètre d'interface sur l'interface de basculement
CSCwd62138	Connexions ASA bloquées à l'état d'inactivité lorsque DCD est activé
CSCwd62859	Vulnérabilité de déni de service des VPN SSL/TLS Cisco ASA et FTD AnyConnect
CSCwd62915	Les utilisateurs interdomaines avec des caractères non-ASCII ne sont pas résolus
CSCwd63221	L'alerte de vidange fréquente d'événements n'est pas déclenchée
CSCwd63580	FPR2100 : Augmentation du temps de convergence de basculement avec l'appareil de sécurité adaptable en mode appareil
CSCwd63722	Mandataire à branche unique FTDv derrière AWS GWLB abandonnés en raison d'une somme de contrôle geneve-invalid-udp-avec toutes les sommes de contrôle 0
CSCwd63961	Les clients AC ne correspondent pas aux règles DAP en raison d'une valeur d'attribut trop élevée
CSCwd64480	Les paquets par le biais des contextes en série dans l'appareil de sécurité adaptable sont abandonnés dans le contexte de la passerelle après la mise à niveau du logiciel
CSCwd64919	FXOS ne fait pas la rotation des journaux PoE
CSCwd65239	Plateformes vFTD ne suivant pas les mesures du processeur/mémoire pour la surveillance de l'intégrité
CSCwd65327	Mise à jour de l'identifiant de validation WR6, WR8, LTS18 et LTS21 dans la couche CCM (séqu. 41)
CSCwd66815	Modifications de Lina pour l'assistance en ligne – Recherche de la source Snort3 dans daq-pdts lors de la gestion du trafic basé sur FQDN
CSCwd66820	Vulnérabilité de contournement de la liste de contrôle d'accès du groupe d'objets Cisco Firepower Management Center

ID du bogue	En-tête :
CSCwd66822	Interfaces du module FDM FPR2k Network sont grisées après la mise à jour 7.1.0
CSCwd68088	ASA FTD : mettre en œuvre différents premiers diffie-hellman TLS en fonction des recommandations de la RFC
CSCwd68745	La console QEMU KVM est bloquée dans la page « Booting the kernel »
CSCwd69139	Recherche de la source Snort 3 sur le flux prune_lru
CSCwd69236	Événement de connexion FMC cesse d'afficher le dernier événement
CSCwd69454	Interfaces de canal de port de l'unité secondaire en attente après le rechargement
CSCwd70490	Indicateur d'état du port du membre du canal de port et état d'adhésion sont inactifs lorsqu'aucun LACPDU n'a été reçu
CSCwd70716	La mise en grappe est désactivée sur tous les nœuds de données après une mise hors/sous tension
CSCwd71254	ASA/FTD peut effectuer une recherche de source et recharger dans la recherche de hachage idfw fqdn
CSCwd72425	Le cœur file internal.cloudapp.net_snort3 est généré lors de la configuration de DST
CSCwd72680	FXOS : temps d'arrêt du FP2100 FTW déclenché par une utilisation élevée du processeur pendant le déploiement de la politique de contrôle d'accès sur Cisco FTD
CSCwd72915	FMC 7.1.0.1 n'envoie pas d'avertissement indiquant que les configurations VPN S2S contiennent un hachage MD5 obsolète lors du déploiement
CSCwd73981	FMC : La page des mises à jour prend plus de 5 minutes à se charger
CSCwd74116	Les tunnels S2S ne s'affichent pas en raison d'un échec du calcul DH causé par la fuite DSID
CSCwd74839	Plus de 30 secondes de perte de données lorsque l'unité rejoint la grappe
CSCwd75738	Les objets texte FlexConfig prédéfinis ne sont pas exportés par l'importation-exportation
CSCwd76622	FTD avec Snort3 peut avoir une corruption de mémoire dans le fichier SNORT avec la même évolutivité du trafic IP
CSCwd76634	L'importation du FMC prend trop de temps
CSCwd76930	Le SN des ventilateurs FPR3110 dans l'étiquette est différent de la sortie de l'interface de ligne de commande de l'inventaire
CSCwd77581	Vulnérabilité de déni de service dans le traitement des messages Cisco ASA et FTD Message ICMPv6
CSCwd78123	Recherche de la source ASA/FTD et rechargement lors de l'établissement de la session VPN IPSec/Ikev2 avec le groupe dh 31 en mode FIPS
CSCwd78624	ASA peut effectuer une recherche de la source et se recharger avec plusieurs messages d'erreur d'entrée/sortie
CSCwd78940	Les pièges ne sont pas générés dans UUT pour la modification de configuration dans le multicontexte

ID du bogue	En-tête :
CSCwd79388	Les incidents d'intrusion ne parviennent pas à migrer de MariaDB vers MonetDB après la mise à niveau de FMC de la version 7.0.3 à la version 7.1.0
CSCwd80343	MI FTD exécutant la version 7.0.4 indique une utilisation de disque élevée
CSCwd80741	Snort abandonne les paquets d'application Bomgar avec la détection précoce des applications activée
CSCwd81384	Échec de la mise à niveau de FMC : 114_DB_table_data_integrity_check.pl, indiquant que Snort2IPSNAPCleanup.pm est introuvable
CSCwd81538	Échec du trafic FTD en raison de l'épuisement du bloc 9344 dans peer_proxy_tx_q
CSCwd81897	Plantage Snort3 observé parfois lors du traitement d'une connexion de flux futur après le rechargement des détecteurs d'applications
CSCwd82235	Recherche de la source LINA sur FPR-1010 sous le nom du fil : update_cpu_usage
CSCwd82801	Snort produit un volume considérable d'événements de paquets – la vue des événements IPS peut afficher « No Packet Information »
CSCwd83141	Filtres CCL/CLU ne fonctionnent pas correctement
CSCwd83613	Vulnérabilité de contournement de l'inspection Snort FTP de plusieurs produits Cisco
CSCwd83956	snort2 ne correspond plus aux règles basées sur l'application SMTP/SMTPS après un certain temps
CSCwd83990	FTD – Snort correspond à un identifiant NAP incorrect pour le trafic
CSCwd84046	L'inscription SCEP de Microsoft ne parvient pas à obtenir le certificat d'identité de l'ASA – Impossible de vérifier PKCS7
CSCwd84133	ASA/FTD peut provoquer une recherche de la source et un rechargement dans le nom de fil 'telnet/ci'
CSCwd84153	ASA/FTD peut rechercher la source et recharger dans le nom de fil « lina »
CSCwd84868	Observation de défaillances devcmd et de recherche de la source lorsque le déchargement de flux n'est pas utilisé.
CSCwd85178	Les licences AWS ASAv PAYG ne fonctionnent pas dans les régions GovCloud.
CSCwd85609	Les FTD exécutant la version 6.6.x affichent comme déconnecté sur le nouveau HM (version 6.7 ou version ultérieure), mais des vérifications sont en cours d'exécution et sont mises à jour
CSCwd85927	Recherche de la source et rechargement lorsque les utilisateurs de webvpn correspondent à la liste d'accès DAP avec des éléments de 36 k
CSCwd86313	Impossible d'accéder à la politique d'accès dynamique
CSCwd86457	Nombre d'objets ne sont pas mis à jour dans les politiques>>>Security Intelligence>>>Liste de blocage
CSCwd86929	Le serveur mandataire traversant ne fonctionne pas avec le trafic HTTPS
CSCwd87227	Utilisation élevée du disque en raison d'une défaillance de la journalisation de process_stdout.log et de process_stderr.log (sans rotation)

ID du bogue	En-tête :
CSCwd88585	Écart d'allocation et de réservation de grappe de pool NAT ASA/FTD entre les unités
CSCwd88641	Modifications de déploiement pour pousser le paquet VDB lite en fonction du modèle d'appareil et du moteur SNORT
CSCwd89349	Mise à jour de l'identifiant de validation WR6, WR8, LTS18 et LTS21 dans la couche CCM (séqu. 42)
CSCwd89811	Le trafic échoue dans la mise en grappe Azure ASAv après un délai d'expiration de secondes
CSCwd90112	Plantage de MariaDB (défaillance de segmentation) lié à la requête netmap
CSCwd91421	ASA/FTD peut faire une recherche de la source et recharger lors du traitement de logging_cfg
CSCwd92804	Voyant DEL du ventilateur clignote en ambre sur FPR2100
CSCwd93376	Les utilisateurs de VPN sans client ne peuvent pas télécharger de fichiers volumineux par le biais du portail WebVPN
CSCwd93465	FMCv 7.2.0 – L'adresse IP de gestion FTD n'est pas correctement mise à jour sur le FMC après la modification de l'adresse IP de gestion FTD
CSCwd93792	Dégradation des performances de SFDataCorrelator impliquant des hôtes avec de nombreuses adresses MAC découvertes
CSCwd94096	Utilisateurs Anyconnect incapables de se connecter lorsque l'appareil de sécurité adaptable utilise un serveur d'authentification et d'autorisation différent
CSCwd94840	SNORT définit le contournement de tunnel pour les paquets codés en Geneve
CSCwd95043	Vulnérabilité de détournement de requêtes côté client pour les services client Cisco ASA et FTD VPN
CSCwd95415	L'appareil en veille passe en état de défaillance en raison d'une défaillance du signal de pulsation de SNORT
CSCwd95436	Recherche de la source dans l'appareil de sécurité adaptable principal lors du redémarrage de l'appareil de sécurité adaptable secondaire
CSCwd95908	Recherche de la source et rechargement ASA/FTD, nom du fil : rtcli async executor process (processus d'exécution asynchrone rtcli)
CSCwd96041	FMC SecureX via serveur mandataire cesse de fonctionner après la mise à niveau vers la version 7.x
CSCwd96493	Link Up visible pendant quelques secondes sur FPR1010 pendant le démarrage
CSCwd96500	FTD : Impossible de configurer le maintien du VPN Web ou la carte de certificats sur FPR3100
CSCwd96755	L'appareil de sécurité adaptable est un rechargement inattendu lors de la sauvegarde
CSCwd96766	FPR41xx/9300 : La lame ne capture pas ou ne journalise pas le signal de redémarrage
CSCwd96790	Taille élevée du fichier de sauvegarde FMC en raison de l'instantané des configurations pour tous les périphériques gérés

ID du bogue	En-tête :
CSCwd96845	Vulnérabilité de contournement de la liste de contrôle d'accès Cisco ASA et FTD AnyConnect
CSCwd97020	ASA/FTD : Échec de l'authentification SAML du fournisseur d'identité externe avec le message de demande incorrecte
CSCwd97276	Les pages d'événements unifiés et d'événements de connexion ne se chargent plus. Cœurs de base de données générés toutes les quelques minutes
CSCwd98070	Impossible d'enregistrer de nouveaux périphériques dans la version FMC 2700 (FMC HA actif)
CSCwe00757	Le tableau de bord de l'état récapitulatif prend plus de 3 minutes à se charger lors de la connexion
CSCwe00828	L'action de blocage interactive ne fonctionne pas lorsque les sites Web sont redirigés vers https
CSCwe00864	Les commandes de licence sont manquantes dans l'unité de données de grappe si la jonction de grappe échoue.
CSCwe03991	Recherche de la source FTD/ASA et rechargement pendant le processus de comptabilité tmatch
CSCwe04437	La collection de top.log.gz dans le dépannage peut être corrompue en raison d'une situation de concurrence
CSCwe05913	Recherche de la source/rechargements FTD – Le traitement des paquets d'erreur Icmp implique snp_nat_xlate_identity
CSCwe06724	L'optimisation des tableaux de base de données ne fonctionne pas pour certains tableaux
CSCwe06828	La synchronisation FMC HA peut se bloquer indéfiniment si aucune réponse de SendUserReloadSGTAndEndpointsEvent
CSCwe07103	FMC : La mise à niveau échoue lors de la vérification de l'intégrité de la base de données en raison d'un grand nombre d'avertissements EO pour « rule_comments »
CSCwe07734	L'appareil de sécurité adaptable Cisco passe en mode de sécurité intégrée après la mise à mise à niveau de FXOS
CSCwe07928	Sur un FMC en nuage, il n'y a aucun moyen d'envoyer des événements à syslog sans les envoyer à SAL/CDO également
CSCwe08729	FPR1120 : Connexions en cours de démontage après le basculement en mode haute disponibilité
CSCwe08908	La configuration d'intégration de Threatgrid n'est pas synchronisée dans le cadre de la synchronisation de FMC à haute disponibilité
CSCwe09074	Aucune option sous le point de confiance ne fonctionne pas lorsque la vérification des CRL échoue
CSCwe09121	Échecs de déploiement de FTD en raison de "snort3.validation.lua:5: '=' attendu près de 'change'"
CSCwe09811	Recherche de la source FTD et rechargement pendant le déploiement de la politique, ajout, suppression ou modification des instructions NAT.

ID du bogue	En-tête :
CSCwe10290	FTD abandonne le trafic GRE de WSA
CSCwe10548	Liaison d'appareil de sécurité adaptable avec LDAP comme méthode d'autorisation avec configuration manquante
CSCwe10670	Filtre de réseau d'identité non supprimé de FTD
CSCwe11119	ASA : recherche de la source et rechargement pendant le traitement des paquets SNMP
CSCwe11189	Le journal monetdb utilise tous les espaces disque sur /Volume
CSCwe11263	Vulnérabilité de téléchargement de fichiers quelconques du logiciel Cisco Firepower Management Center
CSCwe11304	Plantage de Snort sur FTD
CSCwe11727	La purge de l'archive de configuration a échoué pour tous les appareils si un appareil ne comporte aucune version.
CSCwe11902	FTD : Plantage de la haute disponibilité et interfaces en panne sur FPR4200
CSCwe12407	Utilisation élevée de la mémoire Lina en raison d'une fuite de poignées SSL
CSCwe14174	FTD – « show memory top-usage » fournit une valeur inappropriée pour l'allocation de mémoire
CSCwe14417	FTD : La préemption IP SLA ne fonctionne pas, même lorsque la destination devient accessible
CSCwe14514	Recherche de la source ASA/FTD et rechargement de l'unité de secours lors de la suppression des configurations de capture
CSCwe15280	Vulnérabilité de contournement de la politique de contrôle d'accès Snort 3 de Cisco
CSCwe16554	Sessions TLS abandonnées dans certaines conditions après un client Hello fragmenté
CSCwe16620	Le moniteur d'intégrité FMC ne signale pas les alertes pour le module d'état de l'interface
CSCwe17858	Les informations à haute disponibilité de FMC ne sont pas synchronisées de manière fiable avec FTD pour prendre en charge CLOUD_SERVICE
CSCwe18859	Après l'enregistrement du périphérique ou la mise à niveau de FMC, il arrive que les périphériques n'envoient pas d'événements au FMC
CSCwe18974	ASA/FTD peut rechercher la source et recharger dans le nom de fil « CTM Daemon »
CSCwe19286	Vulnérabilité de contournement du moteur de détection Snort 3 et de déni de service du protocole SMB pour Cisco FTD
CSCwe20043	Bloc de mémoire de 256 octets consommé au démarrage si la trame étendue est activée avec FTD sur ASA5516
CSCwe20714	Le trafic est interrompu lorsque l'appareil principal est actif
CSCwe21959	Snort 3 : Processus à l'état D, ce qui entraîne OOM avec le gestionnaire de mémoire jemalloc
CSCwe22176	Mise à jour de l'identifiant de validation WR6, WR8, LTS18 et LTS21 dans la couche CCM (séqu. 43)

ID du bogue	En-tête :
CSCwe22216	Maria DB plante/maintient une UC élevée et ne permet pas aux utilisateurs de se connecter à l'interface graphique et à l'interface de ligne de commande
CSCwe22302	Partition « /opt/cisco/config » est pleine en raison d'une rotation insuffisante du journal du fichier wttmp
CSCwe22386	Les pare-feu inattendus sont rechargés avec recherche de la source.
CSCwe22492	Chargement lent de l'interface utilisateur pour l'affichage du tableau des hôtes
CSCwe22980	La vérification de l'intégrité de la base de données prend plusieurs minutes
CSCwe23039	La fréquence d'interrogation NTP est passée de 5 minutes à 1 seconde, ce qui entraîne de gros fichiers journaux inutiles
CSCwe23139	La haute disponibilité de FTD ne se rompt pas avec l'interface graphique FMC , mais le démarrage haute disponibilité est supprimé des périphériques
CSCwe23801	FTD : De nombreux cœurs SNORT ont été détectés sur l'appareil FPR2100
CSCwe24532	Plusieurs instances des fichiers journaux nvrnm.out ont fait l'objet d'une rotation sous /opt/cisco/platform/logs/
CSCwe24880	L'utilisation de l'authentification par serveur mandataire dans FMC pour les licences intelligentes Cisco échoue après la mise à niveau à la version 7.0.5
CSCwe25025	Impossible de mettre en ligne Netmod 8 x 10 Go
CSCwe25342	ASA/FTD – Comportement de la fuite de mémoire associée au protocole SNMP lorsque le serveur snmp n'est pas configuré
CSCwe25391	Détecteur de service rpc à l'origine de la recherche de la source SNORT en raison de l'adresse universelle étant une chaîne vide
CSCwe26342	Recherche de la source ASA et rechargement citant le nom du fil : asacli/0
CSCwe28094	ASA/FTD peut effectuer une recherche de source et recharger après avoir exécuté la commande « effacer les compteurs » lors de la création des tunnels VPN
CSCwe28726	La commande « app-agent heartbeat » est supprimée lors de la suppression d'un contexte créé
CSCwe29179	CLUSTER (Grappe) : La réponse ICMP arrive à Director avant la demande d'ajout de flux de CLU par le propriétaire de flux.
CSCwe29583	ASA/FTD peut rechercher la source et recharger dans le nom de fil « None » à lua_getinfo
CSCwe29850	ASA/FTD afficher l'implémentation de la commande supérieure chunkstat
CSCwe29952	Cœurs SFDataCorrelator en raison d'une requête de base de données bloquée après 1 heure de délai d'expiration
CSCwe30228	ASA/FTD pourrait effectuer une recherche de la source dans la fonction « snp_fp_l2_capture_internal » en raison de l'indicateur cf_reinject_hide
CSCwe30653	Échec de la mise à niveau de FTD à « 999_finish/999_zz_install_bundle.sh » en raison d'un mauvais certificat de clé

ID du bogue	En-tête :
CSCwe32058	ASA/FTD peut effectuer une recherche de la source et se recharger dans le nom de fil « ci/console » lors de la vérification de la capture de Geneve
CSCwe32448	La modification des paramètres de fenêtre temporelle dans les visualiseurs d'événements de l'interface graphique FMC peut ne pas fonctionner avec FMC intégré à SecureX
CSCwe33819	Snort2 ENH : Utiliser une liste de correspondance de modèles commune pour les modèles CN et SNI dans les applications
CSCwe36176	ASA/FTD : Délai de basculement élevé avec un grand nombre de (sous-)interfaces et le serveur HTTP activé
CSCwe37941	Les fichiers v1_message* et abp* et le signet sxp ne sont pas nettoyés dans user_enforcement lors de l'enregistrement du périphérique
CSCwe38640	Avertissements du gestionnaire d'événements si le syslog facility est CONSOLE
CSCwe39425	2100 : La bascule du commutateur d'alimentation entraîne des arrêts accidentels et une réinitialisation « PowerCycleRequest ».
CSCwe39431	Mise à niveau de FMC : la génération du fichier sftunnel.json par FTD ne vérifie pas les noms en double
CSCwe40463	SA IKEv2 périmée formée lors du traitement simultané de la SA IKE en cas de suppression manquante de l'homologue
CSCwe41336	FDM WM-HA SSH ne fonctionne pas après la mise à niveau de la version 7.2.3 bêta avec l'interface de données comme interface de gestion
CSCwe41898	ASA : temps d'arrêt du FP2100 FTW déclenché par une utilisation élevée du processeur pendant le déploiement de la politique de contrôle d'accès sur FTD
CSCwe42236	FMC : la création du domaine échoue avec l'erreur « Index 'netmap_num' pour la table 'domain_control_info' »
CSCwe44311	FP2100 : Mettre à jour les fichiers asa.log de LINA pour éviter les messages récursifs-<date>.1.gz noms de fichiers tournés
CSCwe44620	Le point d'interrogation dans la description de la NAT entraîne une incompatibilité de configuration sur les membres de données d'une grappe FTD
CSCwe44766	IMS : temps d'arrêt du FP2100 FTW déclenché par une utilisation élevée du processeur pendant le déploiement de la stratégie de contrôle d'accès sur FTD
CSCwe45093	Un utilisateur sans filtre vpn peut obtenir un accès supplémentaire lorsque le remplacement par utilisateur est défini (IKEv2 RAVPN)
CSCwe45222	Les plantages Snort3 sont observés sous le traitement des données Dce2Smb2FileTracker
CSCwe45779	ASA/FTD abandonne le trafic vers BVI si la connexion flottante n'est pas la valeur par défaut en raison d'une contiguïté non valide
CSCwe48378	Lenteur extrême de l'interface utilisateur Web du FMC en raison d'un E/S de disque lourd
CSCwe48432	Impossible d'enregistrer les modifications de la politique de contrôle d'accès en raison d'une erreur interne

ID du bogue	En-tête :
CSCwe49127	La rotation des journaux pour les fichiers process_stderr.log et process_stdout.log peut échouer en raison d'une condition de concurrence
CSCwe50946	État de la liaison de l'interface de gestion non synchronisé entre FXOS et ASA
CSCwe51893	Vulnérabilité de déni de service de l'API Cisco Firepower Management Center
CSCwe52640	Certains conteneurs ont des bordures grisées supplémentaires et certains conteneurs sont de style incorrect
CSCwe54288	Le processus syslog-ng peut se bloquer et entraînerait le module à l'état bloqué
CSCwe54567	Le gestionnaire se désenregistre de lui-même du FTD, afficher gestionnaire affiche « Aucun gestionnaire configuré »
CSCwe55308	Fuite de mémoire dans le MessageService
CSCwe58576	FTD : Le nœud ne rejoint pas la grappe avec « Vérification de l'intégrité détectée que contrôle a quitté la grappe » en raison d'une erreur SSL
CSCwe58700	ASA/FTD : Révision du message d'événement de cluster « Vérification de l'intégrité détectée que contrôle a quitté la grappe »
CSCwe58881	Après la mise à niveau de FMC, le ruban SecureX redirige vers la région du nuage des États-Unis, quelle que soit la région du nuage définie
CSCwe59380	FTD : « timeout floating-conn » ne fonctionne pas comme prévu pour les connexions dépendant du routage VRF
CSCwe59809	CCM, séq. 45 : WR6, WR8, LTS18 et LTS21.
CSCwe59919	Recherche de la source FTD et rechargement sur le nom du fil « NetSnmp Event mib processus »
CSCwe62927	L'échec de l'autorisation de la session DCCSM entraîne plusieurs problèmes dans FMC
CSCwe62971	Échec du déploiement de la politique lors de la tentative de retrait de la configuration du connecteur DNS Umbrella
CSCwe62997	Recherche de la source ASA/FTD dans snp_tracer_format_route
CSCwe63232	ASA/FTD : Vérifier que les états de déchargement de flux dans la grappe sont identiques
CSCwe63316	Pri-Active FMC ne déclenche PAS l'enregistrement de la tâche pour que FTD configure le gestionnaire en veille
CSCwe64043	Listes de contrôle d'accès Cisco ASA et FTD non installées lors du rechargement
CSCwe64404	ASA/FTD peut faire une recherche de la source et un rechargement
CSCwe64542	Processus python TID bloqués à 100 % CPU
CSCwe64557	ASA : Empêcher la configuration du module SFR sur les plateformes non prises en charge
CSCwe64563	La commande « neighbor x.x.x.x ha-mode graceful-restart » supprimée lors de la suppression d'un contexte créé

ID du bogue	En-tête :
CSCwe65245	Les périphériques de la gamme FP2100 peuvent utiliser une mémoire excessive si le taux d'interrogation SNMP est très élevé
CSCwe65492	KP Génération de fichiers noyau non valides qui ne peuvent pas être décodés 7.2.4-64
CSCwe65516	show xlate n'affiche pas les entrées xlate pour les interfaces internes (nlp_int_tap) après l'activation de ssh.
CSCwe66132	ASA/FTD peut rechercher la source et recharger dans le nom de fil « lina »
CSCwe69833	Vulnérabilité de contournement du filtre IP de géolocalisation Snort 3 pour Cisco Firepower Threat Defense Software
CSCwe70378	Connexions non répliquées sur le FTD de secours
CSCwe70558	FTD : impossible d'exécuter des commandes à l'invite de l'interface de ligne de commande
CSCwe70721	Le déploiement est bloqué en raison d'une erreur de validation de prédéploiement d'un point terminal invalide
CSCwe71220	Plantage FTD dans le nom de fil : traitement CP
CSCwe71284	ASA/FTD peut faire une recherche de la source et recharger dans le nom de fil « DATAPATH-3-21853 »
CSCwe71672	Déploiement sélectif annulant les configurations de routage
CSCwe71673	Déploiement sélectif pour la suppression des configurations de préfiltre
CSCwe72535	Connexion impossible au FTD par l'authentification externe
CSCwe73116	Accès croisé : Le ping ICMP pour accéder à la gestion ifc sur VPN est interrompu
CSCwe73240	FMC manque d'espace lorsque Snort envoie un nombre considérable de journaux de paquets
CSCwe74059	logrotate ne compresse pas les fichiers sur les appareils de sécurité adaptables Cisco 9.16 ou sur FTD 7.0.
CSCwe74290	Pourriel SFDataCorrelator vu dans /var/log/messages
CSCwe74328	AnyConnect : les appareils portables ne sont pas en mesure de se connecter lorsque le balayage d'hôtes est activé
CSCwe75018	Les recommandations de règles Snort 2 augmentent considérablement le nombre de règles désactivées
CSCwe75124	Le FMC mis à niveau n'a pas marqué les FTD avec le correctif rapide comme faible enregistrement - échec de la synchronisation HA du FMC
CSCwe75207	Un taux élevé de mises à jour de cartes réseau peut entraîner des retards et des arriérés importants dans le traitement des événements
CSCwe81946	Espace disque vFMC plein en raison de 40 Go de fichiers /var/lib/mysql/undo*
CSCwe83061	La mise à niveau de FMC à partir de FMC actif-principal échoue avec le message « Installation échouée : découverte d'homologue incomplète ».
CSCwe83069	Corriger la valeur d'utilisation de la mémoire Snort3

ID du bogue	En-tête :
CSCwe83478	La cible d'élagage doit prendre en compte la mémoire allouée à partir du fil élagué
CSCwe83812	Pourriel du journal SFDataCorrelator lorsque la cartographie du réseau est complète
CSCwe84079	asa_snmp.log n'est pas soumis à la rotation, ce qui entraîne une taille de fichier volumineuse
CSCwe87591	Catégorie d'URL SSL/TLS du logiciel Cisco FTD et vulnérabilité du contournement du moteur de détection Snort 3 et du DOS
CSCwe87873	Exigence : L'utilitaire de rotation des journaux doit gérer la rotation du fichier asa-appagent.log
CSCwe88808	Interface utilisateur du FMC bloquée après la vérification de la compatibilité
CSCwe89030	L'attribut du numéro de série du DN du sujet du certificat doit être considéré comme nom d'utilisateur
CSCwe89731	Notification de fausse alarme envoyée par le démon pour panne de service.
CSCwe90095	La fonctionnalité de nom d'utilisateur à partir de certificat ne peut pas extraire l'attribut de courriel
CSCwe90334	ID d'instance manquant dans unified_events-2.log
CSCwe91674	Mserver redémarre fréquemment
CSCwe91719	Obtenir « Inconnu » pour plusieurs champs SSL lorsque l'état est Ne pas déchiffrer (Suite de chiffrement non prise en charge)
CSCwe91900	FTD – Message répété dans les journaux à partir des fichiers publication de traitement de sftunnel
CSCwe93202	API REST FXOS : Impossible de créer un trousseau de clés de type « ecdsa ».
CSCwe93885	Échec du déploiement de FDM après la mise à niveau de VDB et de SRU
CSCwe97277	Recherche de la source et rechargement de l'appareil de sécurité adaptable observé lors d'une mise à niveau transparente pendant l'exécution du trafic VPN
CSCwe98146	Cœurs Snort3 observés dans certaines conditions avec le trafic
CSCwe98687	Logiciel Cisco FTD pour la vulnérabilité DoS des règles d'inspection de Cisco Firepower, série 2100
CSCwf00417	FTD : Impossible de traiter un site Web TLS1.2 avec une identité de serveur TLS avec des erreurs SSL générées par le client
CSCwf01051	en veille à l'état désactivé après QP-MI HA 7.0.3 à 7.2.4-126, APPLY_APP_CONFIG_APPLICATION_FAILURE
CSCwf06377	Définition du délai d'expiration de pulsation à 6 secondes pour les périphériques Firepower 4100 et 9300
CSCwf06818	Vulnérabilité de contournement de la politique de fichiers d'archive chiffrée du logiciel Cisco Firepower Threat Defense
CSCwf07030	La page de liste des appareils de mise à niveau prend plus de 15 minutes pour se charger entièrement avec 25 FTD enregistrés

ID du bogue	En-tête :
CSCwf10486	Filtre de réseau d'intégration ISE n'acceptant pas plusieurs réseaux séparés par des virgules
CSCwf11004	Impossible de se connecter avec « information » et « débogage ».
CSCwf14411	getting wrong destination zone on traffic causing traffic to match wrong AC rule (erreur de zone de destination sur le trafic, ce qui fait correspondre le trafic à la mauvaise règle AC)
CSCwf19761	Cœurs SFDC sur la configuration FTD-HA en raison de fils bloqués dans la bibliothèque clamav
CSCwf19853	Erreurs FATALES dans DBcheck en raison de colonnes manquantes dans le tableau eventdb
CSCwf24124	Le processus SFDataCorrelator se bloque très fréquemment sur le FMC.
CSCwf28592	Dans certains scénarios spécifiques, l'optimiseur d'objets peut entraîner le déploiement de règles incorrectes sur le périphérique
CSCwf31176	Vulnérabilité de script intersite du logiciel Cisco Firepower Management Center
CSCwf36674	Vulnérabilité de script intersite dans FMC
CSCwf60584	Surveillance de l'intégrité pour ne pas collecter les statistiques de routage pour FTD
CSCwf63210	Vulnérabilité de l'injection de commande du logiciel Cisco Firepower Management Center
CSCwf63215	Vulnérabilité de traversée de chemin d'accès du logiciel Cisco Firepower Management Center
CSCwf66773	Les commentaires disparaissent des règles d'accès lorsque la règle est copiée dans ou hors de la politique d'accès.
CSCwf67791	Images manquantes dans le fichier sf.xml
CSCwf76945	Les données des paquets sont toujours abandonnées après la mise à niveau
CSCwf85307	Les remplacements de politique IPS [Snort 3] ne fonctionnent pas sur les politiques de prévention des intrusions en chaîne
CSCwh16571	La flèche de navigation permettant d'accéder aux onglets Événement, Priorité et Classification ne fonctionne pas.
CSCwh72699	Amélioration : FMC devrait présenter un avertissement lors de la configuration des paramètres de haute disponibilité de moins d'une seconde pour FTD
CSCwh75924	Une vulnérabilité a été trouvée dans MariaDB. Une analyse de port OpenVAS sur les ports 3306
CSCwi22178	avec l'identité du serveur TLS, la mise en correspondance d'URL donne la priorité au certificat CN sur SNI
CSCwm40822	L'URL doit être mise à jour dans la section de filtrage d'URL.

Bogues résolus dans la version 7.2.3.1

Dernière mise à jour du tableau : 18-04-2023

Tableau 37 : Bogues résolus dans la version 7.2.3.1

ID du bogue	En-tête :
CSCwe53746	La vitesse et le duplex du Firepower 1010E sont définis sur « auto » sur le FMC, le déploiement échoue

Bogues résolus dans la version 7.2.3

Dernière mise à jour du tableau : 27/02/2023

Tableau 38 : Bogues résolus dans la version 7.2.3

ID du bogue	En-tête :
CSCwd09341	Plusieurs fichiers de journalisation n'ont aucun octet en raison d'un échec de journalisation
CSCwd87227	Les fichiers journaux de processus FTD peuvent remplir le disque et entraîner des événements de panne du système et bloquer la capacité de connexion des utilisateurs
CSCwc37695	En plus de l'injection de commande shell c_rehash identifiée dans CVE-2022-1292

Bogues résolus dans la version 7.2.2

Dernière mise à jour du tableau : 30-11-2020

Tableau 39 : Bogues résolus dans la version 7.2.2

ID du bogue	En-tête :
CSCwc10241	Déconnexion cérébrale de la haute disponibilité suite à une mise à niveau ou au redémarrage du périphérique

Bogues résolus dans la version 7.2.1

Tableau 40 : Bogues résolus dans la version 7.2.1

ID du bogue	En-tête :
CSCvo17612	Affichage de messages d'erreur en cas d'échec de la récupération des objets de la base de données
CSCvw82067	Blocs ASA/FTD 9344 supprimés en raison d'un volume élevé de trafic fragmenté
CSCvx24207	Objet FQDN contenant des adresses IPv4 et IPv6 Installer uniquement les entrées IPv6
CSCvx68586	Impossible de se connecter à l'interface utilisateur/SSH sur FMC, la connexion à la console ne demande pas de mot de passe

ID du bogue	En-tête :
CSCvy24180	Ensemble de variables par défaut manquant sur FMC
CSCvy50598	Table BGP ne supprime pas la route connectée lorsque l'interface tombe en panne
CSCvy99348	Commande Shutdown qui redémarre l'appareil FP1k au lieu de l'éteindre.
CSCvz36903	Recherche de la source et rechargement de l'appareil de sécurité adaptable lors de l'allocation d'un nouveau bloc pour le paquet Keepalive de la grappe
CSCvz69729	Des processus clients instables peuvent entraîner la recherche de la source LINA zmqio sur FTD
CSCwa08640	MonetDB plante en raison d'une erreur de taille de fichier
CSCwa59907	Recherche de la source observée par LINA sur le nom du fil « snmp_client_callback_thread »
CSCwa72528	La fonctionnalité de formulaire de nom d'utilisateur ne fonctionne pas avec l'option SER
CSCwa75966	ASA : Rechargement et recherche de la source dans le nom du fil : fil du serveur mandataire de licorice avec défaillance de page : adresse non mappée
CSCwa85492	Réponse de recherche d'URL avec deux catégories
CSCwa89347	Impossible d'ajouter un objet au groupe de réseau sur FMC
CSCwa97917	ISA3000 dans une boucle de démarrage après le cycle d'alimentation
CSCwa99171	Date du châssis et de l'application revient au 1er janvier 2010 après le redémarrage
CSCwb01633	Journaux absents dans FXOS pour diagnostiquer la cause première de l'échec de la génération du fichier d'affichage technique
CSCwb05291	Vulnérabilité d'exécution de code arbitraire côté client dans Cisco ASDM et le logiciel ASA
CSCwb06847	ASA/FTD peut entraîner une recherche de la source et un rechargement dans le nom du fil « DATAPATH-9-11543 »
CSCwb08393	Échec du déploiement de la politique SSL lors de l'utilisation de caractères spéciaux dans les noms de règles SSL
CSCwb12465	Autotests FIPS doivent être exécutés lorsque le mode CC est activé - fichiers manquants
CSCwb13294	Mise à jour de l'identifiant de validation WR8, LTS18 et LTS21 dans la couche CCM (séqu. 25)
CSCwb17963	Impossible d'identifier le mécanisme de limitation de débit dynamique et ne respectant pas la limite de messages par seconde au serveur syslog
CSCwb19648	Les requêtes SNMP pour crasLocalAddress ne renvoient pas les adresses IP attribuées pour les tunnels SSL/DTLS.

ID du bogue	En-tête :
CSCwb19664	Blocage de programmes malveillants faux positifs déclenchés après la mise à niveau à la version 7.0.1
CSCwb20926	FDM : Échec du déploiement des politiques après la mise à niveau en raison de politiques IKEv1 inutilisées
CSCwb38406	Mises à jour de GeoDB dans un environnement multidomaine nécessitent un déploiement manuel de politique
CSCwb41361	Mise à jour de l'identifiant de validation WR8, LTS18 et LTS21 dans la couche CCM (séqu. 26)
CSCwb49416	Recherche de la source du snmpd sur les appareils de sécurité adaptables Cisco et sur les cœurs dans une unité active
CSCwb51821	Erreurs d'utilisation du disque sur l'appareil Firepower Azure en raison de fichiers unifiés de sauvegarde volumineux dans le répertoire ngfw
CSCwb53172	FTD : Les tunnels IKEv2 se rabattent toutes les 24 heures et des fichiers d'archive cryptographiques sont générés
CSCwb53328	Recherche de la source et rechargement ASA/FTD causés par le processus Smart Call Home sch_dispatch_to_url
CSCwb54791	Le serveur DHCP de l'appareil de sécurité adaptable Cisco ne parvient pas à lier l'adresse réservée aux appareils Linux
CSCwb58007	CVE-2022-28199 : évaluation pour FTDv et ASAv
CSCwb59619	PM doit redémarrer le gestionnaire de disques après avoir créé un disque RAM pour que DM soit au courant du disque RAM
CSCwb65447	FTD : Les cœurs AAB ne sont pas complets et ne sont pas décodés
CSCwb65718	FMC est bloqué lors du chargement de la page des objets SI
CSCwb67040	Recherche de la source et rechargement de FP4112 4115 sur le nom de fil : netfs_thread_init
CSCwb68642	ASA – Recherche de la source sur le fil : SXP CORE
CSCwb69503	ASA impossible de configurer aes128-gcm@openssh.com lorsque FIPS est activé
CSCwb71460	ASA – Recherche de la source sur le fil : fover_parse et déclenché par les fonctions liées à snmp
CSCwb73248	FW – Recherche de la source dans la minuterie infra / minuterie netflow
CSCwb74357	Aucune rotation des fichiers journaux pour la partition opt_cisco_platform_logs dans FXOS
CSCwb74571	PBR ne fonctionne pas en mode routé ASA avec membres de la zone

ID du bogue	En-tête :
CSCwb76129	Certains modèles SSL non détectés après l'installation de VDB 356 ou d'une version ultérieure
CSCwb76423	L'appareil de sécurité adaptable plante sur fp2100 lors de la vérification de la liste de révocation de certificats
CSCwb79812	RIP affiche tous les utilisateurs Anyconnect connectés et ne correspond pas à la carte de routage pour la redistribution
CSCwb80559	FTD décharge les paquets étiquetés SGT bien qu'il ne devrait pas
CSCwb80862	Le serveur mandataire ASA/FTD traite tout trafic lors de l'utilisation de l'objet « tout » intégré dans la destination traduite
CSCwb82796	Le pare-feu ASA/FTD peut rechercher la source et recharger lors de la destruction des tunnels IKE
CSCwb83388	Recherche de la source de l'ASA HA actif/en veille observé tous les deux mois environ.
CSCwb83691	Recherche de la source et rechargement d'ASA/FTD en raison de la capture initiée à partir du FMC
CSCwb84638	Amélioration du gestionnaire de ports / LACP pour enregistrer les événements de journalisation lors des redémarrages en raison d'événements externes
CSCwb85633	La sortie Snmpwalk de la mémoire ne correspond pas à l'affichage de la mémoire ou de l'affichage des détails de la mémoire
CSCwb85822	Échec de déploiement lors de la collecte des politiques.
CSCwb86118	TPK ASA : L'appareil peut être bloqué lors de la copie ftp sur le disque
CSCwb86339	Échec de la validation du réseau ACP – Impossible d'analyser ip – Impossible d'appeler la méthode « binip » - Espace vide
CSCwb86565	Échec de la mise à niveau de FMC en raison d'une incompatibilité du nombre d'entrées entre /etc/passwd et /etc/shadow
CSCwb87498	Recherche de la source de Lina et rechargement pendant le traitement de la mise à jour de la route EIGRP.
CSCwb88651	Vulnérabilité de fuite de clé privée Cisco ASA et FTD Software RSA
CSCwb88887	snp_fp_vxlan_encap_and_grp_send_common : échec de recherche d'adj. bp->l3_type = 8, message inner_sip
CSCwb89004	FMC DBcheck.pl bloqué à « Vérification de mysql.rna_flow_stats_template par rapport au schéma actuel »
CSCwb89187	Flex Config allow – « timeout icmp-error hh:mm:ss »
CSCwb90074	ASA : validation de la redirection SFR en mode mixte avec contextes multiples

ID du bogue	En-tête :
CSCwb90105	La mise à niveau vers la version 7.2 sur FTDv pour Nutanix est bloquée après le redémarrage
CSCwb90532	Recherche de la source ASA/FTD et rechargement sur la fonction associée à la NAT nat_policy_find_location
CSCwb91101	Le seuil de l'interface SNMP ne se déclenche pas correctement lorsque le trafic envoyé à l'interface est d'environ 4 Gbps
CSCwb92376	Le daemon syslog-ng de FMC ne parvient pas à démarrer si la fonction de journalisation est définie à ALERT
CSCwb92583	La mise à niveau avec une grande quantité d'espace disque non surveillé peut entraîner l'échec de la mise à niveau et le blocage du périphérique
CSCwb92709	Nous ne pouvons pas surveiller l'interface par l'intermédiaire de « snmpwalk » une fois que l'interface est supprimée du contexte.
CSCwb93932	Recherche de la source ASA/FTD et rechargement avec vérification des services de minuterie
CSCwb94190	Arrêt progressif de l'appareil de sécurité adaptable lors de l'application des ACL avec la fonction de référence de transfert et FIPS activés.
CSCwb94312	Impossible d'appliquer les paramètres SSH à l'appareil de sécurité adaptable version 9.16 ou ultérieure
CSCwb95112	La politique de prévention des intrusions affiche la dernière modification par l'administrateur, même si les modifications sont apportées par un autre utilisateur
CSCwb95787	FPR1010 – Aucun ARP sur l'interface VLAN du port du commutateur après l'événement portmanager DIED
CSCwb97251	ASA/FTD peut effectuer une recherche de la source et recharger dans le nom de fil SSH
CSCwb97486	FPR3100 : les ports à fibre optique 25 G peuvent afficher une liaison sur certains ports à fibre optique uniquement compatibles avec le 1/10G
CSCwc01155	La nouvelle interface utilisateur d'ACP ne se charge pas si des valeurs littérales d'adresse IP d'emplacement sont saisies manuellement dans cette politique
CSCwc02416	Ne pas se réabonner aux rubriques ISE après certains problèmes de connectivité ISE.
CSCwc02488	ASA/FTD peut rechercher la source et recharger dans le nom de fil : 'None'
CSCwc02700	Les paquets fragmentés sont abandonnés lorsque l'unité quitte la grappe
CSCwc03069	Les données internes de l'interface data0/0 sont activées/désactivées à partir de l'interface de ligne de commande, mais ascendantes/désactivées à partir de l'interrogation SNMP
CSCwc03296	La mise à niveau échoue lors de l'utilisation du service DDNS avec un utilisateur et un mot de passe

ID du bogue	En-tête :
CSCwc04162	Valeurs TTL à l'origine de la retransmission des paquets
CSCwc04187	Plantage de la surveillance sur FP1000 lors de l'établissement d'un tunnel VPN SSL AnyConnect très lourd
CSCwc05132	Impossible de désactiver l'option « Récupérer dans le centre de gestion »
CSCwc07015	Plantage de snort3 en raison du pointeur NULL dans l'évaluation du client Hello de TLS
CSCwc08374	Adresse MAC du NIC de la carte réseau Azure ASA pour Gigeth 0/1 et 0/2 arrête de fonctionner après l'ajout d'interfaces
CSCwc09414	ASA/FTD peut rechercher la source et recharger dans le nom de fil 'ci/console'
CSCwc10483	ASA/FTD – Recherche de la source dans le nom du fil : appAgent_subscribe_nd_thread
CSCwc10792	ASA/FTD IPSEC débogue le motif manquant pour le changement d'adresse d'homologue et la suppression de la minuterie
CSCwc10900	La recherche dans le nuage d'URL si elle est activée sur le FMC peut ne pas fonctionner sur les périphériques nouvellement enregistrés.
CSCwc11597	Recherches de la source ASA après la mise à niveau de SFR à la version 6.7.0.3
CSCwc11663	Retour en arrière et rechargement de l'appareil de sécurité adaptable lors de la modification de la politique d'inspection du DNS par l'intermédiaire du CSM ou de l'interface de ligne de commande
CSCwc12652	ACL du plan de contrôle non fonctionnel après la mise à niveau vers la version 9.18(1) ou 7.2.0-82 Firepower
CSCwc13017	Recherche de la source et rechargement de FTD/ASA à l'adresse ../inspect/proxy.h:439
CSCwc13382	Le trafic DCERPC est abandonné après la mise à niveau vers SNORT3 en raison de la fermeture du flux parent
CSCwc13994	ASA – Restaurer sans supprimer la nouvelle configuration pour une configuration d'interface après la sauvegarde
CSCwc14885	FMC déconnecte l'utilisateur lors de la modification d'une page en arrière-plan
CSCwc15530	La fonction de journal système « ALERTE » doit être modifiée sur FDM, car elle n'est plus prise en charge par syslog-ng
CSCwc18218	Les fichiers de base de données sur le disque deviennent plus volumineux que prévu pour certains tableaux fréquemment mis à jour
CSCwc18312	les commandes « show nat pool cluster » exécutées dans les scripts EEM entraînent la recherche de la source et le rechargement
CSCwc23075	Mise à niveau vers MariaDB 10.5.16 pour obtenir des correctifs de failles de sécurité

ID du bogue	En-tête :
CSCwc23356	ASA/FTD peut rechercher la source et recharger dans le nom de fil « DATAPATH-20-7695 »
CSCwc23695	ASA/FTD ne peut pas analyser l'UPN à partir du champ SAN du certificat de l'utilisateur
CSCwc24422	SSLVPN AC avec authentification par certificat et échec DAP si le certificat de la machine du client a un objet vide
CSCwc24906	Recherche de la source et rechargement ASA/FTD sur l'ID de thread : 1637
CSCwc25275	Interface utilisateur de la politique AC : Impossible de rechercher les règles pendant le chargement des règles
CSCwc25451	Nouvelle interface utilisateur de la politique AC : L'ajout d'une règle dans une catégorie entraîne une erreur d'index
CSCwc28334	Vulnérabilité de fuite de clé privée Cisco ASA et FTD Software RSA
CSCwc28532	9344 Fuite de blocage en raison d'un trafic GRE fragmenté sur le traitement du flux interne de l'interface défini en ligne
CSCwc28660	Snort3 : Le montage de NFSv3 peut échouer pour le trafic via FTD
CSCwc28928	ASA : Les débogages SLA ne s'affichent pas sur les sessions VTY
CSCwc29591	Échec des mises à jour rétrospectives de la disposition des fichiers en raison de valeurs d'événement incorrectes dans les tableaux d'événements de fichier
CSCwc30487	Utilisation élevée du disque non géré sur le Firepower 2110
CSCwc32246	NAT64 traduit toutes les adresses IPv6 en 0.0.0.0/0 lorsque le sous-réseau d'objet 0.0.0.0 0.0.0.0 est utilisé
CSCwc37196	FPR3100 : Le réseau netmod 8x1G en cuivre peut indiquer par erreur un micrologiciel obsolète au démarrage
CSCwc40322	L'intégration de FMC sur site à CDO à l'aide de SecureX échoue en raison d'une erreur d'authentification de l'utilisateur
CSCwc40850	Échec de l'authentification FMC avec SecureX Orchestration
CSCwc41590	Échec de mise à niveau et échec de démarrage de l'instance d'application avec l'erreur « CSP_OP_ERROR. CSP signature verification error. » (erreur de vérification de la signature CSP)
CSCwc41661	FTD Plusieurs fichiers journaux avec une taille de zéro octets.
CSCwc59953	Plantage de Snort3 avec TLS 1.3
CSCwc65907	snort3 se bloque dans le gestionnaire de plantage, ce qui peut entraîner une interruption prolongée pendant un plantage de SNORT

ID du bogue	En-tête :
CSCwc69376	Problèmes de performances après la mise à niveau de la v7.2 en raison d'un nombre excessif de tables de partition intrusionevent
CSCwc76658	SFDataCorrelator ne parvient pas à démarrer après la mise à niveau de <7.1 à >=7.1.0 en raison de compliance.rules "session_both"
CSCwc88583	Le déploiement échoue avec une erreur de mode Snort3IntrusionPolicy non valide. Prend en charge uniquement en ligne et en ligne-test

Bogues résolus dans la version 7.2.0.1

Tableau 41 : Bogues résolus dans la version 7.2.0.1

ID du bogue	En-tête :
CSCwb88651	Vulnérabilité de fuite de clé privée Cisco ASA et FTD Software RSA
CSCwb93932	Recherche de la source ASA/FTD et rechargement avec vérification des services de minuterie
CSCwc28334	Vulnérabilité de fuite de clé privée Cisco ASA et FTD Software RSA

Bogues résolus dans la version 7.2.0

Tableau 42 : Bogues résolus dans la version 7.2.0

ID du bogue	En-tête :
CSCwa70008	Les certificats expirés entraînent l'échec des mises à jour de Security Intelligence
CSCvz67001	Échec des sauvegardes d'événements FMC vers des cibles de stockage SSH distantes
CSCvy46482	Groupe d'objets de service redondant créé lors de l'utilisation de l'ACL cryptographique dans le VPN S2S.
CSCwb22359	Amélioration du gestionnaire de ports/LACP pour éviter les faux redémarrages et l'augmentation des événements de journalisation
CSCwb64551	Échec de la sauvegarde FMC – Code de défaillance de la sauvegarde Monetdb 102
CSCwa00038	La corruption du disque se produit lorsque la partition /mnt/disk0 est pleine et que la lame est redémarrée
CSCwa40223	Vulnérabilité de script intersite du logiciel Cisco Firepower Management Center
CSCwa45656	Échec de l'application de la licence SLR sur les périphériques gérés
CSCwa34110	FMC devrait prendre en charge les configurations DST de l'hémisphère Sud
CSCwa32956	Les événements de connexion ne sont pas envoyés au centre de gestion Cisco Firepower Management Center en raison d'une situation de concurrence dans le déploiement

ID du bogue	En-tête :
CSCvz40765	Le graphique UC FMC affiche le nombre incorrect de cœurs Snort et System
CSCvy19453	Problèmes de performance de SFDataCorrelator impliquant des événements de nouvel hôte redondants avec uniquement des adresses MAC
CSCwa12688	Échec de l'installation de l'objet d'authentification extérieure RADIUS sur Cisco FTD en raison de tentatives non valides
CSCwb40001	Retards longs lors de l'exécution des commandes SNMP
CSCwa95694	Cœurs Snort générés par intermittence lorsque la politique SSL est activée sur le module ASA-SFR
CSCwa08262	Les utilisateurs AnyConnect avec des politiques de groupe mappées prennent les attributs du GP par défaut sous le groupe de tunnel
CSCvz27235	Vulnérabilité de déni de service de plusieurs produits Cisco dans Snort
CSCvz14377	Perte de l'administrateur et d'autres utilisateurs à partir de MySQL DB et EO
CSCvz80981	SNMPv3 ne fonctionne pas pour les modules SFR exécutant la version 7.0
CSCvz68336	Déchiffrement SSL ne fonctionne pas en raison d'une seule connexion sur plusieurs paires en ligne
CSCvx75683	La sortie « show cluster info trace » est dépassée par les messages « tag does not exist (balise n'existe pas) »
CSCwa79604	Exécution infinie des tâches dans la liste des tâches
CSCwa43497	Blocages de chemin de données observés lors de l'envoi de PMTU ICMP pour AnyConnect-SSL
CSCvx59252	FXOS n'effectue pas la rotation des fichiers journaux pour l'interface de gestion
CSCwa15093	Contrôle de la politique d'accès Effacer le nombre d'accès générant l'erreur 403 : Accès refusé
CSCwa06608	Le basculement WM 1010 à haute disponibilité ne réussit pas lorsque nous activons le basculement en secondaire.
CSCvz41761	FMC ne permet pas de créer une clé secrète d'authentification EIGRP en utilisant le caractère \$
CSCwb46481	SNMPv3 ne fonctionne pas après la mise à niveau de FMC
CSCvq29993	FPR2100 UNIQUEMENT – Fuite de blocs pérenne du trafic de blocs de mémoire et de trous noir de taille 80, 256 et 1550
CSCwa70323	Impossible de pousser des domaines supplémentaires > 1024 caractère, dans le cadre de l'attribut personnalisé sous Anyconnect VPN
CSCwb46340	Échec de la mise à niveau d'Elektra lors de la mise à niveau

ID du bogue	En-tête :
CSCvz77050	Il arrive que des échecs de déploiement de politique soient signalés comme réussis.
CSCvz61456	La mise à niveau logicielle sur l'application ASA peut échouer sans raison apparente
CSCwb16561	Interface graphique FMC ne charge pas les politiques de prévention des intrusions
CSCwa74984	Impossible d'ouvrir l'onglet des détails d'accès de FMC -> configuration après la mise à niveau de FMC
CSCvz89713	Le processus FMC dbsrv16 présente une utilisation élevée de la CPU après la mise à niveau de FMC
CSCvz73583	FTD n'envoie pas les informations d'authentification au serveur mandataire lors du téléchargement de VDB et de GeoDB.
CSCvz02027	Mettre à jour l'hôte à partir de l'URL s'il n'est pas disponible dans le paquet pour arrêter la recherche dans le nuage pour les demandes HTTP d'hôte nul
CSCwa84862	Impossible de supprimer ou de modifier les objets de liste d'accès standard dans FMC
CSCvz03524	Échec de la vérification de la révocation d'OCSP en raison d'une demande sha256 au lieu de sha1
CSCwa85340	Impossible de générer le PDF avec la politique d'accès ayant de gros objets imbriqués
CSCwa27488	Échec de l'importation avec l'erreur « n'est pas un tableau »
CSCwa89689	Serveur hello effectué sur TLS supprimé par FTD après avoir activé la « détection précoce des applications » avec snort3
CSCwb50405	Recherche de la source ASA/FTD dans la fonction de hachage chiffré
CSCvz08588	Alarme d'utilisateur non reconnu pour les utilisateurs du domaine d'identité découvert
CSCug96057	Les appareils de la même catégorie sont classés avec plusieurs noms de catégorie
CSCwb11939	Modification de l'adresse MAC ASA/FTD lors du traitement des paquets fragmentés avec INSPECT activé
CSCvz09109	La capture de l'interface CCL de la grappe affiche des paquets complets, bien que seuls les en-têtes soient configurés
CSCwb20940	FMC : ajouter des vérifications de validation pour la combinaison SSL/Snort3/NAP en mode de détection
CSCvz90654	L'unité de basculement FTD ne rejoint pas la haute disponibilité en raison d'un « échec de la progression de l'état de la haute disponibilité en raison de l'expiration du délai de la synchronisation de l'application »
CSCwa55868	Échec du déploiement de la politique QP vFTD avec snort2 avec une variable de paquet non définie
CSCvz78331	Échec de l'interrogation SNMP après une recreation d'image

ID du bogue	En-tête :
CSCwa70482	ASDM sur la fenêtre contextuelle MAC supprime le paquet hostscan/CSD
CSCvz62517	L'installation de la SRU devrait valider les fichiers une fois terminée
CSCwa41918	L'inspection SSL peut avoir un comportement inattendu lors de l'éjection des certificats
CSCvz29656	Recherche d'événement de connexion FMC entraînant une utilisation élevée de la mémoire pour index.cgi
CSCvz78548	Impossible de charger la page Appareils --> Certificats
CSCwa79676	FPR1010 en HA émet des alertes de tempête de diffusion pour plusieurs interfaces
CSCwa81395	Un corps de demande soigneusement conçu peut entraîner un débordement de la mémoire tampon dans le...
CSCwa81143	Impossible d'enregistrer le filtre de politique d'application. L'onglet de sauvegarde est bloqué et se charge continuellement.
CSCvy75131	Les capteurs/interfaces supprimés à l'occasion ne sont pas retirés des zones de sécurité
CSCvz73957	FTD arrête de générer les ID Syslog 430002 et 430003 avec les cœurs du gestionnaire d'événements
CSCvy24921	SNMPv3 : L'ID de moteur SNMP change après chaque modification de configuration
CSCvy24435	L'interface graphique de FMC est accessible par un mot de passe expiré lors de l'utilisation de .cgi avec https://FMCIP/login.cgi
CSCwa97423	La restauration du déploiement entraîne une brève perte du trafic en raison de l'ordre des opérations
CSCvz89106	Vulnérabilité d'exfiltration de données d'identification de nom de serveur de plusieurs produits Cisco
CSCwa11088	L'ordre des règles d'accès est automatiquement modifié lorsque vous essayez de le modifier avant l'actualisation ou le chargement de la page
CSCvz62261	Impossible de restreindre l'accès des utilisateurs lors de l'utilisation d'ASDM
CSCwb19387	Le sondage SNMP ASA échoue et affiche « Impossible de répondre à cette demande maintenant. Veuillez réessayer plus tard ».
CSCwa98983	Échec de la mise à niveau 7.1.0.1-25 sur KP-HA à 800_post/901_reapply_sensor_policy.pl
CSCwa83078	Snort3 : les sessions reprises non déchiffrées peuvent échouer
CSCwb42846	UC de l'instance Snort bloquée à 100 %
CSCwb59218	Impossible d'enregistrer les critères du terminal DAP en tant que « Désactivé »
CSCvx90486	Dans certains cas, snmpwalk pour ifXTable peut ne pas renvoyer d'interfaces de données

ID du bogue	En-tête :
CSCvz76745	Croissance de la mémoire SFDDataCorrelator avec des événements malveillants en nuage
CSCvz13564	Firepower 2100 : La configuration de la liste d'accès ssh-access-list est perdue après la mise à niveau
CSCwa35179	Le certificat VPN FTD AC est perdu lors des rechargements
CSCwb84225	Évaluation des CVE OpenJDK pour l'API REST ASDM et ASA
CSCwa38996	Grand nombre de messages répétitifs dans snmpd.log, ce qui entraîne une taille de journal énorme
CSCvy80380	Augmentation de l'utilisation du disque /var/tmp dans le châssis FPR4150-ASA
CSCwb01126	La configuration du serveur DNS est perdue si elle est configurée par le biais de la page VPN d'accès à distance sur FDM 7.1.0
CSCwa68004	FMC 7.0 FlexConfig a bloqué le temps de vieillissement de la table d'adresses mac pour FTD transparent sans alternative
CSCwb29126	Impossible d'utiliser le trait de soulignement (_) dans la configuration du domaine AD principal du domaine de FMC
CSCwa99370	Config. ASDM :DAP manquant le type d'attributs AAA (Radius/LDAP)
CSCwa89560	Modification de la règle NAT après la recherche de règles change l'ordre des règles
CSCvy33501	Paire de basculement FDM – le nouveau sVTI IPsec SA configuré n'est pas synchronisé en mode veille. FDM affiche la haute disponibilité n'est pas synchronisée
CSCwa75077	Objets de plage temporelle mal remplis dans les règles de préfiltre
CSCwb07319	Les balises de droit contiennent un caractère non valide.
CSCwa91070	Cgroup déclenchant oom-k pour le processus de sauvegarde
CSCwa45369	L'exécution des commandes semble entraîner un nouveau processus zombie
CSCwb44048	Le taux d'événements sur le tableau de bord de surveillance de l'intégrité de FMC affiche des valeurs extrêmement élevées
CSCvz72467	Déni de service pour le protocole de découverte des logiciels Cisco FXOS et NX-OS
CSCwb37999	Nom des variables personnalisées à l'origine de l'échec de la validation de Snort3
CSCvz73315	Les événements de connexion ne sont pas vus sur FMC, SFDDataC ne traite pas les événements de to_import dir
CSCwb21704	FDM : ajouter des vérifications de validation pour la combinaison SSL/Snort3/NAP en mode de détection
CSCwb32841	Les instructions NAT (toutes, toutes) dans l'état de l'interface de basculement entraînent des événements de déconnexion cérébrale

ID du bogue	En-tête :
CSCvz79930	Les fichiers Snort3 .dmp et crashinfo ne sont pas gérés par diskmanager
CSCwa51867	FDM IKEv2 S2S PSK ne se déploie pas correctement (passage de PSK asymétrique à PSK symétrique)
CSCwa39683	Fichier de journal inondé par les messages ssl_policy log_error lorsque le débogage SSL est activé
CSCwa25033	Trame de données HTTP/2 imprévue causant une défaillance secondaire
CSCwa39680	Snort arrête de traiter les paquets lorsque le débogage du déchiffrement SSL est activé - Snort2
CSCvz24238	Vulnérabilité de script intersite du centre de gestion Cisco Firepower Management Center
CSCwa31373	Les règles ACP en double sont générées sur FMC 6.6.5 après la copie de la règle.
CSCwa43311	Blocage et abandon de paquet Snort, avec téléchargement de fichier de plus grande taille (1 G)
CSCwa32286	Mise à jour de l'ID de validation WR6, WR8 et LTS18 dans la couche CCM (sprint 125, seq 21)
CSCwb24039	Recherche de la source ASA et rechargement lors du routage
CSCwa46963	Sécurité : CVE-2021-44228 -> vulnérabilité Log4j 2
CSCwb06543	Augmenter le niveau de journalisation pour diagnostiquer les événements de redémarrage inattendu du processus LACP
CSCwb43018	Implémenter l'API SNP pour vérifier si c et ip appartiennent à l'interface HA LU ou CMD
CSCvz76652	L'URL d'URI du mandataire pour le filtrage d'URL (service beaker) comprend des chaînes d'utilisateur et de mot de passe codées
CSCvz51570	FDM : Incompatibilité de nom d'interface de gestion entre les unités HA et l'interface utilisateur/l'interface de ligne de commande de FDM
CSCvz66236	Mauvais comportement de seuil de « -1 » après la configuration de Type : les deux pour une règle spécifique
CSCwb59488	Échec de la recherche de la source ASA/FTD dans l'allocation de mémoire
CSCwa42350	L'installation/la mise à niveau de l'appareil de sécurité adaptable échoue en raison d'une erreur interne « Ressources disponibles non mises à jour par module »
CSCvz32593	QP4110 et QW4115 à l'état désactivé avec erreur de synchronisation d'application de CD est Rsync n'est pas activé sur le périphérique actif
CSCwa76621	Processus HM arrêté sur FTD 1120

ID du bogue	En-tête :
CSCvy67765	FTD VTI signale TUNNEL_SRC_IS_UP faux bien que l'interface source soit opérationnelle
CSCvz02076	Le rechargement de Snort expire ce qui entraîne son redémarrage
CSCwa32628	Plantage de SFDataCorrelator à AddFileToPendingHash() en raison d'une situation de concurrence
CSCwa07390	Configuration uniquement FMC : Le fichier téléchargé de flux SI ne correspond pas à la somme de contrôle attendue
CSCwa97910	Le rapport d'événement de connexion affiche le même périphérique deux fois
CSCwb48686	ASAV ne démarrera pas sur REDHAT KVM sous Dell PowerEdge R650
CSCwa27822	Le processus lina reste à l'état démarré après une mise à niveau majeure de FTD vers la version 6.7 ou la version 7.0
CSCwb11325	nullPointerException pendant 100_ftd_onbox_data_import.pl entraîne l'échec de la mise à niveau de 7.0.0 à 7.1.0
CSCwb32721	Les ID de journal système 725021 et 725022 ne sont pas répertoriés comme des ID valides
CSCwa35596	Les périphériques enregistrés peuvent ne pas être présents sur le FMC en veille en raison d'un échec de synchronisation des fichiers de classe AnyConnect HostScan
CSCwa26353	snort3 - La politique ne devient pas modifiée après la mise à jour du LSP - lorsque seules les politiques de prévention des intrusions personnalisées sont utilisées
CSCvz70539	Le processus Loggerd est arrêté en raison d'un message OOM sous un taux de journalisation élevé
CSCvr97157	Amélioration : Amélioration du comportement en cas d'échec du déploiement sur FTD géré par FDM
CSCwb28047	FMC – « Réception du fil abandonnée avec une exception : stoï », ce qui fait basculer pxGrid
CSCwa21016	Vulnérabilité de déni de service de Cisco Firepower Threat Defense Software DNS Enforcement
CSCwb16663	Impossible de configurer la Politique d'analyse de réseau (NAP) sous l'onglet Avancé de la politique CA
CSCvy82655	API REST – La création de règles CA en bloc échoue avec l'entité non traitable 422
CSCvt76856	Si une connexion au serveur Smart satellite utilise un certificat, elle ne peut pas être rétablie.
CSCwa77396	Impossible de créer des alertes de moniteur dans FMC

ID du bogue	En-tête :
CSCvy50797	Le déploiement de la politique peut échouer si les paramètres de la plateforme contiennent DH group1 pour SSL
CSCvz91266	FXOS – Un uri-path de demande spécialement conçu peut pousser mod_proxy à transférer la demande à un serveur d'origine
CSCwa86210	Lorsque PM désactive Mysqld, il faut parfois plus de temps que prévu pour s'arrêter complètement.
CSCwa72641	URL incorrectement extraite pour les URL autosignées TLS v1.2 lorsque la « détection précoce des applications » est activée
CSCwa85138	Plusieurs problèmes liés aux diagnostics de validation transactionnels
CSCwa48169	Recherche de la source ASA/FTD sur la fonction netsnmp_handler_check_cache
CSCvx24470	FTD/FDM : Sessions de VPN d'accès à distance déconnectées après chaque déploiement si le port personnalisé pour le VPN d'accès à distance est configuré
CSCvz96440	FMC ne doit pas créer d'archivage pour les périphériques NGIPS
CSCwa04171	FMC génère et supprime inutilement les commandes AAA pour le domaine
CSCwa31488	La haute disponibilité FDM ne peut pas être créée en utilisant EtherChannel comme interface de basculement.
CSCvy65200	Caractères aléatoires affichés dans le champ DNSQuery pour des requêtes spécifiques.
CSCwb31699	Le serveur principal joue un rôle actif après le rechargement
CSCwb19648	Les requêtes SNMP pour crasLocalAddress ne renvoient pas les adresses IP attribuées pour les tunnels SSL/DTLS.
CSCvz70688	L'origine des informations par défaut est configurée en premier, puis la commande de talon n'est pas autorisée pour la configuration
CSCwa03732	Le déploiement est bloqué à la phase de génération de l'instantané pendant le déploiement
CSCvz69699	L'interface utilisateur de FMC peut devenir inaccessible en raison de fuites de connexion dans la base de données interne
CSCwa69279	FMC : Impossible de configurer AnyConnect MTU pour la politique de groupe avec uniquement le protocole IKEv2 activé
CSCwa62167	CIAM : Apache-http-server CVE-2021-44790 et CVE-2021-44224
CSCwa48849	ssl unexpected behavior with resumed sessions (comportement inattendu du protocole SSL avec la reprise des sessions)
CSCwa52215	Téléchargement du micrologiciel déclenche l'oscillation du canal de port de données
CSCvy99218	La version VDB ne doit pas être mise à jour en cas d'échec

ID du bogue	En-tête :
CSCwa50145	La connexion à l'interface utilisateur du capteur FPR8000 crée un utilisateur Shell avec des privilèges de base
CSCvz19634	La mise à niveau du logiciel FTD peut échouer à l'adresse 200_pre/505_revert_prep.sh
CSCwa85220	Échec de l'autorisation dans le pont DCCSM lors de l'enregistrement de l'appareil.
CSCwa21061	Échec de la mise à niveau de FTD sur 800_post/100_ftd_onbox_data_import.sh
CSCwa98853	Erreur F0854, le module RSA de la clé FDM n'est pas valide
CSCvv59757	Échec de la génération du rapport d'événement FMC s'il y en a déjà un en cours d'exécution
CSCvz66506	Recherche de la source ADI continue et rechargement sur FPR2100 enregistrés dans FMC à haute disponibilité
CSCvz85234	Les fonctionnalités ALERT, AUDIT, CLOCK et KERN ne fonctionnent pas dans l'envoi du journal d'audit à syslog à partir de FMC.
CSCvz84733	Les paquets LACP par le biais de l'ensemble en ligne sont abandonnés en silence
CSCvx89451	La commande d'arrêt ISA3000 redémarre le système et n'arrête pas le système.
CSCvz43325	FMC actif ne dérégistre pas les capteurs après l'interruption de la haute disponibilité
CSCwa55974	FMC doit effectuer une interruption de toutes les sessions de configuration précédentes avant d'appliquer une nouvelle version
CSCwa77083	Les renseignements sur l'hôte sont manquants lorsque les zones de sécurité sont configurées dans les règles de détection du réseau
CSCwa42596	ASA avec la configuration SNMPv3 observe des rechargements inattendus avec les noyaux snmpd
CSCwb84638	Amélioration du gestionnaire de ports / LACP pour enregistrer les événements de journalisation lors des redémarrages en raison d'événements externes
CSCwa31139	FMC ne vérifie pas le chevauchement d'adresses IP avec l'interface de basculement FTD
CSCwa08084	La restauration de l'appareil matériel FMC se termine avec une erreur « Condition de défaillance inconnue »
CSCwb08828	FP1010 vlan d'accès au port de commutation en état actif/actif, mais ne transmet pas le trafic
CSCvz53993	Blocage aléatoire de paquets par Snort dans le flux SSL
CSCvv82681	La lecture du registre de l'horloge instable RTC entraîne l'erreur « watchdog: BUG: soft lockup - CPU#0 stuck » sur la console
CSCwa67145	Le téléchargement de domaine échoue si l'un des groupes est supprimé sur AD

ID du bogue	En-tête :
CSCvu82743	Règles de l'ID du Générateur Snort 3 désactivées après le rechargement de Snort
CSCwa17918	Impossible de décocher l'option Toujours annoncer la route par défaut pour OSPF
CSCvp15884	Alertes d'intégrité du SI du FMC : liste des URL du SI et flux du système - faux-positifs en cas d'échec
CSCwa55418	multiple db folders current-policy-bundle after deployment with anyconnect package before upgrade (plusieurs dossiers db current-policy-bundle après le déploiement avec le paquet anyconnect avant la mise à niveau)
CSCvz35787	Indicateur de flux OVER_SUBSCRIBED trompeur pour le flux intermédiaire FTD
CSCwa53088	snort 2 ssl-debug files may not be written (fichiers débogage ssl snort 2 peuvent ne pas être écrits)
CSCwa29956	Le message « Configuration de l'interface a changé sur le périphérique » peut s'afficher après la mise à niveau de Cisco FTD
CSCwa60574	Recherche de la source et rechargement de l'appareil de sécurité adaptable sur la fonction snp_ha_trans_alloc_msg_muxpuf_space
CSCwb38669	Nom de la politique LACP défini à Null après la mise à niveau à la version 7.1.0.90 (2.11.1.154) sur FPR1150
CSCwb08644	Recherche de la source ASA/FTD et rechargement au niveau IKEv2 à partir du test de longue durée évolutif S2S + AC-DTLS + SNMP
CSCvz97196	Impossible de créer un objet Flexconfig avec l'attribut de nommage ldap pager car le pager est bloqué.
CSCwb09219	ASA/FTD : OCSP peut ne pas fonctionner après la mise à niveau en raison d'un « certificat de signataire introuvable »
CSCwa85297	Les VLAN du canal de port internes multi-instances peuvent être mal programmés, ce qui entraîne une perte de trafic
CSCvz25197	Vulnérabilité de déni de service de plusieurs produits Cisco dans Snort
CSCug44895	Échec du chargement lorsqu'un plus grand nombre de curseurs sont renvoyés par le PAS
CSCwa67209	FMC peut désactiver la négociation automatique pour les canaux de port avec membres en fibre optique SFP de 1 Gb/s après la mise à niveau de FTD
CSCwb24101	Le journal système Loggerd a des horodatages incorrects, par exemple bien avant FirstPacketSecond
CSCwa51862	Échec des téléchargements de LSP lors de l'utilisation du serveur mandataire
CSCwa78082	La recherche d'incident d'intrusion FMC produit des résultats incohérents

ID du bogue	En-tête :
CSCwa80040	Échec de configuration du NFS du FMC après la mise à niveau de la version 6.4.0.4 à la version 7.0.1
CSCvz52430	Interface utilisateur FDM inaccessible 503 Service non disponible en raison de cinq serveurs DNS configurés
CSCwb07981	Recherche de la source : le FTD en veille redémarre et génère des informations de plantage et un cœur lina sur le nom du fil cli_xml_server
CSCwb02316	Erreur « Non stop forwarding non supported on 'I' » lors de la configuration de l'adresse MAC
CSCwa92883	Échec du déploiement à la phase 2 avec une erreur d'instantané du domaine
CSCvz61463	FP9k SM-44 6.7.0.2. CPU élevé sur les cœurs vdp de Radware après la mise à niveau
CSCwa55142	SNORT3 / SSL / Verdict de DND final lorsqu'il y a une règle de bas de DND supplémentaire, au lieu du DND normal
CSCvy88460	Impossible d'ajouter des objets d'authentification RADIUS supplémentaires après la mise à niveau vers la version 6.7.0
CSCvz72771	L'appareil de sécurité adaptable/FTD peut effectuer une recherche de la source et se recharger. « c_assert_cond_terminate » dans la trace de la pile
CSCwb07908	FTD/ASA en veille envoie des requêtes DNS avec l'IP de la source 0.0.0.0
CSCwa13721	Échec de la mise à niveau de FTD géré par FDM lorsque le chiffrement personnalisé est sélectionné dans les paramètres SSL
CSCvj08826	Le fichier FMC ibdata1 peut devenir volumineux
CSCwa14524	Noyaux Snort dans pfts_sftls_daq_acquire avec SSL activé
CSCwb43629	La licence et la règle comptent les données de télémétrie générées incorrectement pour les périphériques gérés à haute disponibilité
CSCwa31508	Échec du déploiement continu sur l'appareil QW-4145
CSCwa79905	La génération du rapport de politique NAT FMC n'enregistre pas les règles tous les 51*x
CSCwa90660	Le téléchargement d'utilisateur/groupe de domaine FMC n'effectue pas la tâche
CSCwb56718	Le déploiement de la politique échoue avec une erreur : la mise à jour de la règle est en cours d'exécution, mais il n'y a aucune mise à jour en cours.

Pour de l'assistance

Guides de mise à niveau

Dans les déploiements On-Prem Firewall Management Center, le On-Prem Firewall Management Center doit exécuter une version de maintenance (le troisième chiffre) identique ou plus récente que celle de ses périphériques gérés. Mettez d'abord le On-Prem Firewall Management Center à niveau, puis les périphériques. Utilisez le guide de mise à niveau de la version que vous utilisez *actuellement*, et non celui de votre version cible.

Tableau 43 : Guides de mise à niveau

Observations	Guide de mise à niveau	Lien
On-Prem Firewall Management Center	version On-Prem Firewall Management Center que vous utilisez <i>actuellement</i> .	https://cisco.com/go/fmc-upgrade
Firewall Threat Defense avec On-Prem Firewall Management Center	version On-Prem Firewall Management Center que vous utilisez <i>actuellement</i> .	https://cisco.com/go/ftd-fmc-upgrade
Firewall Threat Defense avec gestionnaire d'appareil	version Firewall Threat Defense que vous utilisez <i>actuellement</i> .	https://cisco.com/go/ftd-fdm-upgrade
Firewall Threat Defense avec Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)	Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).	https://cisco.com/go/ftd-cdfmc-upgrade

Guides d'installation

Si vous ne pouvez pas ou ne souhaitez pas effectuer de mise à niveau, vous pouvez installer les versions majeures et de maintenance les plus récentes. C'est ce que l'on appelle la *recréation d'image*. Cette procédure ne peut pas s'appliquer à un correctif. Installez la version majeure ou de maintenance appropriée, puis appliquez le correctif. Si vous procédez à une recréation d'image vers une version antérieure de Firewall Threat Defense sur un périphérique FXOS, une recréation d'image complète est nécessaire, y compris pour les périphériques où le système d'exploitation et le logiciel sont combinés.

Tableau 44 : Guides d'installation

Observations	Guide d'installation	Lien
On-Prem Firewall Management Center matériel	Guide de démarrage du modèle de On-Prem Firewall Management Center matériel.	https://cisco.com/go/fmc-install
Firewall Management Center Virtual	Guide de démarrage pour le Firewall Management Center Virtual	https://cisco.com/go/fmcfv-quick

Observations	Guide d'installation	Lien
Firewall Threat Defense matériel	Guide de démarrage ou de recréation d'image relatif à votre modèle de périphérique.	https://cisco.com/go/ftd-quick
Firewall Threat Defense Virtual	Guide de démarrage de votre version Firewall Threat Defense Virtual.	https://cisco.com/go/ftdv-quick
FXOS pour Cisco Firepower 4100/9300	Guide de configuration de votre version de FXOS, chapitre <i>Gestion des images</i> .	https://cisco.com/go/firepower9300-config
FXOS pour Cisco Firepower 1000/2100 et Secure Firewall 3100	Guide de dépannage, chapitre <i>Procédures de recréation d'image</i> .	Guide de dépannage Cisco FXOS pour le Firepower 1000/2100 et Secure Firewall 3100/4200 avec Firepower Threat Defense

Autres ressources en ligne

Cisco fournit des ressources en ligne suivantes pour télécharger de la documentation, des logiciels et des outils, pour rechercher des bogues et pour ouvrir des demandes de service. Utilisez ces ressources pour installer et configurer le logiciel Cisco, ainsi que pour résoudre les problèmes techniques.

- Documentation : <https://cisco.com/go/threatdefense-72-docs>
- Site d'assistance et de téléchargement Cisco : <https://cisco.com/c/en/us/support/index.html>
- Outil de recherche de bogues de Cisco : <https://tools.cisco.com/bugsearch/>
- Service de notification de Cisco : <https://cisco.com/cisco/support/notifications.html>

Vous devez posséder un identifiant utilisateur et un mot de passe sur Cisco.com pour pouvoir accéder à la plupart des outils du Site d'assistance et de téléchargement Cisco.

Communiquez avec Cisco

Si vous ne pouvez pas résoudre un problème à l'aide des ressources en ligne répertoriées ci-dessus, communiquez avec : Centre d'assistance technique Cisco (TAC)

- Courriel Centre d'assistance technique Cisco (TAC) : tac@cisco.com
- Composez le Centre d'assistance technique Cisco (TAC) (Amérique du Nord) : 1.408.526.7209 ou 1.800.553.2447
- Appelez le Centre d'assistance technique Cisco (TAC) (monde entier) : [Contacts d'assistance Cisco dans le monde](#)

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2022–2025 Cisco Systems, Inc. Tous droits réservés.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d'incohérence, la version anglaise du présent contenu prévaudra.