Notes de mise à jour pour Cisco Secure Firewall ASA série 9.19(x)

Dernière modification : 2025-08-11

Notes de mise à jour pour Cisco Secure Firewall ASA série 9.19(x)

Ce document contient des informations sur la version 9.19(x) du logiciel ASA.

Remarques importantes

- **Aucune prise en charge dans l'ASA 9.19(1) et les versions ultérieures pour les Firepower 4110, 4120, 4140, 4150 et les modules de sécurité SM-24, SM-36 et SM-44 pour le Firepower 9300.**L'ASA 9.18(x) est la dernière version prise en charge.

Configuration système requise

ASDM nécessite un ordinateur doté d'une unité centrale avec au moins 4 cœurs. Un nombre réduit de cœurs peut entraîner une utilisation élevée de la mémoire.

Compatibilité ASA et ASDM

Pour en savoir plus sur les exigences et la compatibilité du logiciel et du matériel ASA/ASDM, y compris la compatibilité des modules, consultez Cisco Cisco Secure Firewall ASA Compatibility (Cisco > Compatibilité).

Compatibilité VPN

Pour la compatibilité VPN, consultez Supported VPN Platforms, Cisco ASA 5500 Series (Plateformes VPN prises en charge, série Cisco ASA 5500).

Nouvelles fonctionnalités

Cette section énumère les nouvelles fonctionnalités de chaque version.

Remarque Les messages syslog nouveaux, modifiés et obsolètes sont répertoriés dans le guide des messages syslog.

Nouvelles fonctionnalités dans l'ASA 9.19(1)

Publication : 29 novembre 2022

Fonctionnalités	Description
Caractéristiques de la plateforme	
Secure Firewall 3105	Nous avons présenté l'ASA pour le Secure Firewall 3105.
Solution virtuelle ASA Auto Scale avec équilibreur de charge de la passerelle Azure	Vous pouvez maintenant déployer la solution virtuelle ASA Auto Scale avec équilibreur de charge de la passerelle sur Microsoft Azure. Consultez les fonctionnalités Interfaces pour en savoir plus.
Caractéristiques du pare-feu	
Soutien aux groupes de service du réseau	Vous pouvez désormais définir un maximum de 1 024 groupes de services réseau.
Fonctionnalités de haute disponibilité et d'évolutivité	
Suppression des propos tendancieux	Les commandes, les sorties de commande et les messages syslog qui contenaient les termes « Master » (maître) et « Slave » (esclave) ont été remplacés par « Control » (contrôle) et « Data » (données). Commandes nouvelles/modifiées : **cluster control-node**, **enable as-data-node**, **prompt**, **show cluster history**, **show cluster info**
Regroupement virtuel d'ASA sur Amazon Web Services (AWS)	L'ASA virtuel prend en charge le regroupement d'interfaces individuelles pour un maximum de 16 nœuds sur AWS. Vous pouvez utiliser la mise en grappe avec ou sans équilibreur de charge de la passerelle AWS.
Fonctionnalités de routage	
Prise en charge du redémarrage progressif de BGP pour IPv6	Nous avons ajouté la prise en charge du redémarrage progressif de BGP pour la famille d'adresses IPv6. Commandes nouvelles/modifiées : Commande existante, étendue à la prise en charge de la famille IPv6 :**ha-mode graceful-restart**
Caractéristiques de l'interface	
Prise en charge virtuelle de l'IPv6 par l'ASA	ASAv pour prendre en charge le protocole réseau IPv6 sur les plateformes du nuage privé et public. Les utilisateurs peuvent désormais : • Activer et configurer une adresse de gestion IPv6 via la configuration day0. • Attribuer des adresses IPv6 à l'aide de méthodes DHCP et statiques.

Fonctionnalités	Description
Proxy jumelé VXLAN pour l'ASA virtuel pour l'équilibreur de charge de la passerelle Azure.	Vous pouvez configurer une interface VXLAN en mode proxy apparié pour l'ASA virtuel dans Azure afin de l'utiliser avec l'équilibreur de charge de la passerelle Azure (GWLB). L'ASA virtuel définit une interface externe et une interface interne sur un seul NIC en utilisant des segments VXLAN dans un serveur mandataire jumelé. Commandes nouvelles/modifiées : **port externe, segment-id externe, port interne, segment-id interne, proxy paired**
La correction d'erreur par défaut (FEC) sur les ports fixes du Secure Firewall 3100 est passée de cl74-fc à cl108-rs pour les émetteurs-récepteurs SR, CSR et LR de 25 Go+.	Lorsque vous définissez le FEC sur Auto sur les ports fixes du Secure Firewall 3100, le type par défaut est désormais défini sur cl108-rs au lieu de cl74-fc pour les émetteurs-récepteurs SR, CSR et LR de 25 Go. Commandes nouvelles/modifiées : **fec**
Caractéristiques de la licence	
Prise en charge de la réservation de licences virtuelles permanentes pour l'ASAv5 sur KVM et VMware	Une nouvelle commande est disponible que vous pouvez exécuter pour remplacer la licence DPP par défaut et demander à Cisco Smart Software Manager (SSM) d'envoyer une licence DPP ASAv5 lorsque vous déployez ASAv avec 2GB RAM sur KVM et VMware. Vous pouvez modifier la même commande en ajoutant la forme <*no*> pour rétablir la licence de l'ASAv5 à la licence DPP par défaut en fonction de la configuration de la mémoire vive.
Fonctions d'administration, de surveillance et de dépannage	
Pile CiscoSSH maintenant par défaut	La pile Cisco SSH est maintenant utilisée par défaut. Commandes nouvelles ou modifiées : **ssh stack ciscossh**
Fonctionnalités du VPN	
Prise en charge de l'interface de bouclage VTI	Vous pouvez désormais définir une interface de bouclage comme interface source pour un VTI. La possibilité d'hériter de l'adresse IP d'une interface de bouclage au lieu d'une adresse IP configurée de manière statique a également été ajoutée. L'interface de boucle avec retour permet de résoudre les échecs de chemin. Si une interface tombe en panne, vous pouvez accéder à toutes les interfaces grâce à l'adresse IP attribuée à l'interface de boucle avec retour. Commandes nouvelles/modifiées : **tunnel source interface**, **ip unnumbered**, **ipv6 unnumbered**
Prise en charge de l'interface de tunnel virtuel dynamique (VTI dynamique)	L'ASA est améliorée grâce à l'ITV dynamique. Un seul VTI dynamique peut remplacer plusieurs configurations de VTI statique sur le concentrateur. Vous pouvez ajouter de nouveaux satellites à un concentrateur sans modifier la configuration du concentrateur. Dynamique VTI prend en charge les rayons dynamiques (DHCP). Commandes nouvelles/modifiées : **interface virtual-Template, ip unnumbered, ipv6 unnumbered, tunnel protection ipsec policy.**
Support VTI pour EIGRP et OSPF	Le routage EIGRP et OSPFv2/v3 est désormais pris en charge sur l'interface du tunnel virtuel. Vous pouvez maintenant utiliser ces protocoles de routage pour partager les informations de routage et pour acheminer le flux de trafic à travers le tunnel VPN basé sur VTI entre les pairs.

Fonctionnalités	Description
TLS 1.3 dans le VPN d'accès à distance.	Vous pouvez désormais utiliser TLS 1.3 pour chiffrer les connexions VPN d'accès à distance. TLS 1.3 ajoute la prise en charge des chiffrements suivants : • TLS_AES_128_GCM_SHA256 • TLS_CHACHA20_POLY1305_SHA256 • TLS_AES_256_GCM_SHA384 Cette fonctionnalité nécessite Cisco Secure Client, version 5.0.01242 ou ultérieure. Commandes nouvelles/modifiées : **sslserver-version, sslclient-version**.
Prise en charge de la double pile pour les clients tiers IKEv2	Secure Firewall ASA prend désormais en charge les demandes d'IP à double pile provenant de clients VPN d'accès à distance tiers IKEv2. Si le client VPN d'accès à distance tiers demande des adresses IPv4 et IPv6, l'ASA peut désormais attribuer les deux versions d'adresses IP à l'aide de plusieurs sélecteurs de trafic. Cette fonction permet aux clients VPN d'accès à distance tiers d'envoyer des données IPv4 et IPv6 par le biais d'un seul tunnel IPsec. Commandes nouvelles/modifiées : **show crypto ikev2 sa, show crypto ipsec sa, show vpn-sessiondb ra-ikev2-ipsec**.
Sélecteur de trafic pour l'interface VTI statique	Vous pouvez maintenant attribuer un sélecteur de trafic à une interface VTI statique. Commandes nouvelles/modifiées : **tunnel protection ipsec policy**.

Mettre à niveau le logiciel

Cette section fournit des informations sur le chemin de mise à niveau et un lien pour terminer la mise à niveau.

Lien de mise à niveau

Pour terminer votre mise à niveau, consultez le guide de mise à niveau de l'ASA.

Chemin de mise à niveau : Appareils ASA

Quelle version dois-je mettre à niveau?

Sur le site d'assistance et de téléchargement Cisco, la version suggérée est marquée d'une étoile d'or. Par exemple :

Illustration 1 : Version suggérée

Affichez votre version actuelle

Pour afficher la version et le modèle actuels, utilisez l'une des méthodes suivantes :

- ASDM : Choisissez **Home** > **Device Dashboard** > **Device Information (Accueil > Tableau de bord des appareils > Informations sur les appareils)**.
- Interface de ligne de commande : Utilisez la commande **show version** .

Directives de mise à niveau

Veillez à vérifier les instructions de mise à niveau pour chaque version entre votre version de départ et votre version d'arrivée. Dans certains cas, vous devrez modifier votre configuration avant de procéder à la mise à niveau, faute de quoi vous risquez de subir une panne.

Pour obtenir des informations sur les problèmes de sécurité de l'ASA et savoir quelles versions contiennent des correctifs pour chaque problème, consultez les ASA Security Advisories (avis de sécurité de l'ASA).

Chemins de mise à niveau

Ce tableau fournit des chemin sde mise à niveau pour l'ASA.

Remarque ASA 9.18 était la version finale pour les Firepower 4110, 4120, 4140 et 4150, et les modules de sécurité SM-24, SM-36 et SM-44 pour le Firepower 9300.

ASA 9.16 était la version finale pour les ASA 5506-X, 5508-X et 5516-X.

ASA 9.14 était la version finale pour les ASA 5525-X, 5545-X et 5555-X.

ASA 9.12 était la version finale pour les ASA 5512-X, 5515-X, 5585-X et ASASM.

ASA 9.2 était la version finale pour l'ASA 5505.

ASA 9.1(x) était la version finale pour les ASA 5510, 5520, 5540, 5550 et 5580.

Tableau 1 : Chemin de mise à niveau

Version actuelle	Version de mise à jour provisoire	Version cible
9,18	—	L'un des éléments suivants : → 9.19
9.17	—	L'un des éléments suivants : → 9.19 → 9.18
9.16	—	L'un des éléments suivants : → 9.19 → 9.18 → 9.17

Version actuelle	Version de mise à jour provisoire	Version cible
9.15	—	L'un des éléments suivants : → 9.19 → 9.18 → 9.17 → 9.16
9.14	—	L'un des éléments suivants : → 9.19 → 9.18 → 9.17 → 9.16
9.13	—	L'un des éléments suivants : → 9.19 → 9.18 → 9.17 → 9.16
9.12	—	L'un des éléments suivants : → 9.19 → 9.18 → 9.17 → 9.16
9.10	—	L'un des éléments suivants : → 9.19 → 9.18 → 9.17 → 9.16 → 9.12
9.9	—	L'un des éléments suivants : → 9.19 → 9.18 → 9.17 → 9.16 → 9.12

Version actuelle	Version de mise à jour provisoire	Version cible
9.8	—	L'un des éléments suivants : → 9.19 → 9.18 → 9.17 → 9.16 → 9.12
9.7	—	L'un des éléments suivants : → 9.19 → 9.18 → 9.17 → 9.16 → 9.12
9.6	—	L'un des éléments suivants : → 9.19 → 9.18 → 9.17 → 9.16 → 9.12
9.5	—	L'un des éléments suivants : → 9.19 → 9.18 → 9.17 → 9.16 → 9.12
9.4	—	L'un des éléments suivants : → 9.19 → 9.18 → 9.17 → 9.16 → 9.12

Version actuelle	Version de mise à jour provisoire	Version cible
9.3	—	L'un des éléments suivants : → 9.19 → 9.18 → 9.17 → 9.16 → 9.12
9.2	—	L'un des éléments suivants : → 9.19 → 9.18 → 9.17 → 9.16 → 9.12
9.1(2), 9.1(3), 9.1(4), 9.1(5), 9.1(6), ou 9.1(7.4)	—	L'un des éléments suivants : → 9.12
9.0(2), 9.0(3) ou 9.0(4)	—	L'un des éléments suivants : → 9.12

Chemin de mise à niveau : ASA sur Firepower 2100 en mode plateforme

Pour afficher la version et le modèle actuels, utilisez l'une des méthodes suivantes :

- ASDM : Choisissez **Home** > **Device Dashboard** > **Device Information (Accueil > Tableau de bord des appareils > Informations sur les appareils)**.
- Interface de ligne de commande : Utilisez la commande **show version** .

Ce tableau fournit des chemins de mise à niveau pour l'ASA sur le Firepower 2100 en mode plateforme. Certaines versions nécessitent une mise à niveau intermédiaire avant de pouvoir passer à une version plus récente. Les versions recommandées sont en **gras**.

Veillez à vérifier les instructions de mise à niveau pour chaque version entre votre version de départ et votre version d'arrivée. Dans certains cas, vous devrez modifier votre configuration avant de procéder à la mise à niveau, faute de quoi vous risquez de subir une panne.

Pour obtenir des informations sur les problèmes de sécurité de l'ASA et savoir quelles versions contiennent des correctifs pour chaque problème, consultez les ASA Security Advisories (avis de sécurité de l'ASA).

Tableau 2 : Chemin de mise à niveau

Version actuelle	Version de mise à jour provisoire	Version cible
9,18	—	L'un des éléments suivants : → **9.19**
9.17	—	L'un des éléments suivants : → **9.19** → **9.18**
9.16	—	L'un des éléments suivants : → **9.19** → **9.18** → 9.17
9.15	—	L'un des éléments suivants : → **9.19** → **9.18** → 9.17 → **9.16**
9.14	—	L'un des éléments suivants : → **9.19** → **9.18** → 9.17 → **9.16** → 9.15
9.13	→ 9.18	L'un des éléments suivants : → **9.19**
9.13	—	L'un des éléments suivants : → **9.18** → 9.17 → **9.16** → 9.15 → 9.14
9.12	→ 9.18	L'un des éléments suivants : → **9.19**

Version actuelle	Version de mise à jour provisoire	Version cible
9.12	—	L'un des éléments suivants : → **9.18** → 9.17 → **9.16** → 9.15 → 9.14
9.10	→ 9.17	L'un des éléments suivants : → **9.19** → **9.18**
9.10	—	L'un des éléments suivants : → 9.17 → **9.16** → 9.15 → 9.14 → 9.12
9.9	→ 9.17	L'un des éléments suivants : → **9.19** → **9.18**
9.9	—	L'un des éléments suivants : → 9.17 → **9.16** → 9.15 → 9.14 → 9.12
9.8	→ 9.17	L'un des éléments suivants : → **9.19** → **9.18**

Version actuelle	Version de mise à jour provisoire	Version cible
9.8	—	L'un des éléments suivants : → 9.17 → **9.16** → 9.15 → 9.14 → 9.12

Chemin de mise à niveau : périphériques logiques ASA pour le Firepower 4100/9300

- FXOS : À partir de FXOS 2.2.2 et les versions ultérieures, vous pouvez effectuer une mise à niveau directement vers n'importe quelle version ultérieure. (FXOS 2.0.1–2.2.1 peut mettre à niveau jusqu'à 2.8.1. Pour les versions antérieures à 2.0.1, vous devez effectuer une mise à niveau à chaque version intermédiaire.) Notez que vous ne pouvez pas mettre à niveau FXOS vers une version qui ne prend pas en charge votre version d'appareil logique actuelle. Vous devrez effectuer la mise à niveau en étapes : mettez à niveau FXOS vers la version la plus élevée qui prend en charge votre appareil logique actuel; mettez à niveau votre périphérique logique vers la version la plus élevée prise en charge avec cette version FXOS. Par exemple, si vous souhaitez effectuer une mise à niveau de FXOS 2.2/ASA 9.8 vers FXOS 2.13/ASA 9.19, vous devrez effectuer les mises à niveau suivantes :

  1. FXOS 2.2 -> FXOS 2.11 (la version la plus élevée qui prend en charge 9.8)
  2. ASA 9.8 -> ASA 9.17 (la version la plus élevée prise en charge par 2.11)
  3. FXOS 2.11 jusqu'à FXOS 2.13
  4. ASA 9.17 -> ASA 9.19

- Défense contre les menaces : Des mises à niveau provisoires peuvent être nécessaires pour défense contre les menaces , en plus des exigences FXOS ci-dessus. Pour le chemin de mise à niveau exact, consultez le centre de gestion guide de mise à niveau de votre version.
- ASA : ASA vous permet de procéder à une mise à niveau directement de votre version actuelle vers toute version supérieure, en notant les exigences FXOS ci-dessus.

Tableau 3 : Compatibilité du Firepower 4100/9300 avec l'ASA et Défense contre les menaces

Version de FXOS	Modèle	Version d'ASA	Défense contre les menacesVersion
2.16	Firepower 4112	9.19 9,18 9.17	**7.6** (recommandé) 7.4 7.3 7.2 7.1
	Firepower 4145 Firepower 4125 Firepower 4115	9.19 9,18 9.17	**7.6** (recommandé) 7.4 7.3 7.2 7.1
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
2.14(1)	Firepower 4112	9.19 9,18 9.17 9.16 9.14	**7.4** (recommandé) 7.3 7.2 7.1 7.0 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	9.19 9,18 9.17 9.16 9.14	**7.4** (recommandé) 7.3 7.2 7.1 7.0 6.6
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		

Version de FXOS	Modèle	Version d'ASA	Défense contre les menacesVersion
2.13	Firepower 4112	**9.19 (recommandé)** 9,18 9.17 9.16 9.14	**7.3** (recommandé) 7.2 7.1 7.0 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.19 (recommandé)** 9,18 9.17 9.16 9.14	**7.3** (recommandé) 7.2 7.1 7.0 6.6
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
2.12	Firepower 4112	**9.18** (recommandé) 9.17 9.16 9.14	**7.2** (recommandé) 7.1 7.0 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.18** (recommandé) 9.17 9.16 9.14 9.12	**7.2** (recommandé) 7.1 7.0 6.6 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.18** (recommandé) 9.17 9.16 9.14 9.12	**7.2** (recommandé) 7.1 7.0 6.6 6.4
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

Version de FXOS	Modèle	Version d'ASA	Défense contre les menacesVersion
2,11	Firepower 4112	**9.17** (recommandé) 9.16 9.14	**7.1** (recommandé) 7.0 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.17** (recommandé) 9.16 9.14 9.12	**7.1** (recommandé) 7.0 6.6 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.17** (recommandé) 9.16 9.14 9.12 9.8	**7.1** (recommandé) 7.0 6.6 6.4
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.10 **Remarque** Pour la compatibilité avec 7.0.2 et 9.16 (3.11) +, vous avez besoin de FXOS 2.10 (1.179) +.	Firepower 4112	**9.16** (recommandé) 9.14	**7.0** (recommandé) 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.16** (recommandé) 9.14 9.12	**7.0** (recommandé) 6.6 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.16** (recommandé) 9.14 9.12 9.8	**7.0** (recommandé) 6.6 6.4
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

Version de FXOS	Modèle	Version d'ASA	Défense contre les menacesVersion
2.9	Firepower 4112	9.14	6.6
	Firepower 4145 Firepower 4125 Firepower 4115	9.14 9.12	6.6 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	9.14 9.12 9.8	6.6 6.4
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2,8	Firepower 4112	**9.14**	**6.6** **Remarque** La version 6.6.1 et ultérieures nécessite FXOS 2.8(1.125) et ultérieures.
	Firepower 4145 Firepower 4125 Firepower 4115	**9.14** (recommandé) 9.12 **Remarque** Firepower 9300 SM-56 nécessite la version ASA 9.12(2) et ultérieures	**6.6** (recommandé) **Remarque** La version 6.6.1 et ultérieures nécessite FXOS 2.8(1.125) et ultérieures. 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.14** (recommandé) 9.12 9.8	**6.6** (recommandé) **Remarque** La version 6.6.1 et ultérieures nécessite FXOS 2.8(1.125) et ultérieures. 6.4 6.2.3
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

Version de FXOS	Modèle	Version d'ASA	Défense contre les menacesVersion
2.6(1.157) **Remarque** Vous pouvez désormais exécuter ASA 9.12 et FTD 6.4+ sur des modules distincts du même châssis Firepower 9300	Firepower 4145 Firepower 4125 Firepower 4115	**9.12** **Remarque** Firepower 9300 SM-56 nécessite ASA 9.12.2 et versions ultérieures	**6.4**
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.12** (recommandé) 9.8	**6.4** (recommandé) 6.2.3
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.6(1.131)	Firepower 9300 SM-48 Firepower 9300 SM-40	**9.12**	Non pris en charge
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.12** (recommandé) 9.8	
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.3(1.73)	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	9.8 **Remarque** 9.8(2.12)+ est requis pour le déchargement de flux lors de l'exécution de FXOS 2.3(1.130)+.	**6.2.3** (recommandé) **Remarque** 6.2.3.16 et ultérieures nécessite FXOS 2.3.1.157 ou ultérieure.
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

Version de FXOS	Modèle	Version d'ASA	Défense contre les menacesVersion
2.3(1.66) 2.3(1.58)	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	9.8 **Remarque** 9.8(2.12)+ est requis pour le déchargement de flux lors de l'exécution de FXOS 2.3(1.130)+.	
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2,2	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.8**	Les versions Défense contre les menaces sont en fin de vie (EoL).
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

Remarque sur les rétrogradations

La rétrogradation des images FXOS n'est pas officiellement prise en charge. La seule méthode prise en charge par Cisco pour rétrograder une version d'image FXOS consiste à effectuer une recréation d'image complète de l'appareil.

Bogues ouverts et résolus

Les bogues ouverts et résolus pour cette version sont accessibles via l'outil de recherche de bogues de Cisco. Cet outil Web vous permet d'accéder au système de suivi des bogues de Cisco, qui conserve les informations sur les bogues et les vulnérabilités de ce produit et d'autres produits matériels et logiciels de Cisco.

Remarque Vous devez avoir un compte Cisco.com pour vous connecter et accéder à l'outil de recherche de bogues de Cisco. Si vous n'en avez pas, vous pouvez vous inscrire pour obtenir un compte. Si vous n'avez pas de contrat d'assistance Cisco, vous ne pouvez rechercher les bogues que par leur numéro d'identification; vous ne pouvez pas effectuer de recherches.

Pour plus de renseignements sur l'outil de recherche de bogues de Cisco, consultez l'aide et FAQ de l'outil de recherche de bogues.

Bogues ouverts dans la version 9.19(x)

Le tableau suivant répertorie une sélection de bogues ouverts au moment de la publication de cette note de mise à jour.

Identifiant	En-tête :
CSCwc58458	L'interface AWS C5N-4Xlarge 10g dispose de 4 files d'attente RX avec GENEVE et bâti grand format activées

Bogues résolus dans la version 9.19(1)

Le tableau suivant répertorie les bogues résolus au moment de la publication de cette note de mise à jour.

Identifiant	En-tête :
CSCvv82681	La lecture du registre de l'horloge instable RTC entraîne l'erreur « watchdog: BUG: soft lockup - CPU#0 stuck » sur la console
CSCvw23514	Mettre à jour la documentation de dépannage de FXOS pour fournir des détails sur l'isolement des défaillances potentielles de matériel SSD
CSCvx54562	Mémoire de surdébit système élevée sur FTD
CSCvx99172	Les disques SSD de modèle M500IT sur 4100/9300 peuvent ne plus répondre après 3,2 ans de service
CSCvy99348	Commande Shutdown qui redémarre l'appareil FP1k au lieu de l'éteindre.
CSCvz34289	Dans certains cas, la transition vers un proxy allégé ne fonctionne pas pour les flux Ne pas déchiffrer
CSCvz52785	L'interface de gestion oscille toutes les 13 minutes après la mise à niveau de 9.12 à 9.14.2.15
CSCvz68713	La réservation de licences PLR pour ASAv5 requiert ASAv10
CSCvz69729	Des processus clients instables peuvent entraîner la recherche de la source LINA zmqio sur FTD
CSCvz90712	9.17/Fuite ou épuisement rare de 256 blocs, surallocation de 1 550 blocs
CSCvz94217	Version de départ de l'instance d'application est ignorée et définie comme version en cours après copie de la configuration
CSCwa16257	le basculement échoue dans le FTD secondaire lorsque l'interface de boucle avec retour est configurée
CSCwa38996	Grand nombre de messages répétitifs dans snmpd.log, ce qui entraîne une taille de journal énorme
CSCwa48169	Recherche de la source ASA/FTD sur la fonction netsnmp_handler_check_cache
CSCwa52215	Téléchargement du micrologiciel déclenche l'oscillation du canal de port de données

Identifiant	En-tête :
CSCwa55772	Rechargement inattendu dans FPR 4100 avec la raison « Reset triggered due to HA policy of Reset »
CSCwa69303	L'ASA s'exécutant sur la plateforme SSP génère une erreur critique « [FSM:FAILED]: sam:dme:MgmtIfSwMgmtOobIfConfig »
CSCwa76822	Réglage du contrôle de limitation du flux sur les destinations syslog-ng
CSCwa77777	Ajout de plus de journaux à l'infrastructure de surveillance
CSCwa82850	Le basculement ASA ne détecte pas d'incompatibilité de contexte avant de déclarer que le nœud de jonction est « en veille »
CSCwa85297	Les VLAN du canal de port internes multi-instances peuvent être mal programmés, ce qui entraîne une perte de trafic
CSCwa90735	FTD/FXOS – Les fichiers ASAconsole.log ne fonctionnent pas, ce qui entraîne un espace disque excessif utilisé dans /ngfw
CSCwa96920	ASA/FTD peut rechercher la source et recharger dans le processus Lina
CSCwa99171	Date du châssis et de l'application revient au 1er janvier 2010 après le redémarrage
CSCwa99932	ASA/FTD bloqué après le plantage et le redémarrage
CSCwb00871	ENH : réduire la latence dans log_handler_file pour réduire la surveillance en cas d'évolutivité ou de sollicitation
CSCwb01633	Journaux absents dans FXOS pour diagnostiquer la cause première de l'échec de la génération du fichier d'affichage technique
CSCwb02689	FXOS devrait vérifier la strate de l'horloge de référence plutôt que la strate de l'horloge locale du serveur NTP
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
CSCwb05148	Vulnérabilité du déni de service SNMP des logiciels Cisco ASA et FTD
CSCwb18602	crontab -e impossible de trouver l'‘éditeur
CSCwb22359	Amélioration du gestionnaire de ports/LACP pour éviter les faux redémarrages et l'augmentation des événements de journalisation
CSCwb25809	Passage unique – Recherche de la source en raison d'un ifc obsolète
CSCwb27099	FXOS : Interopérabilité tierce entre le serveur Cisco Ciela et un châssis Firepower
CSCwb28123	Le déploiement de FTD à haute disponibilité échoue avec l'erreur « Le déploiement a échoué en raison d'une modification de version majeure sur le périphérique »

Identifiant	En-tête :
CSCwb31551	Lorsque le paquet entrant contient un en-tête SGT, FPR2100 ne peut pas distribuer correctement selon le tuple 5
CSCwb40662	Amélioration : Le FCM devrait inclure une option de modification de « link debounce time (délai de l'antirebond du lien) de l'interface
CSCwb48166	Mise à niveau de FXOS à la version 2.11 est bloquée
CSCwb57524	Échec de la mise à niveau de FTD - Espace disque insuffisant en raison des anciens ensembles FXOS dans la partition distribuable
CSCwb57615	La configuration de la liste d'accès au pbr avec le numéro de ligne a échoué.
CSCwb57988	Recherche de la source dans smConLogger causé par une fuite de mémoire
CSCwb58007	CVE-2022-28199 : évaluation pour FTDv et ASAv
CSCwb62059	Connexion impossible au FTD par l'authentification extérieure après la mise à niveau
CSCwb63827	DoS du logiciel Cisco Adaptive Security Appliance et du logiciel Firepower Threat Defense
CSCwb66382	ASAv – Le bloc 9344 n'est pas créé automatiquement après l'activation du bâti grand format, ce qui rompt le protocole OSPF MD5
CSCwb70030	MIO : aucun redémarrage de la lame pendant CATERR si la gravité de la défaillance est non grave ou si le capteur CATERR est différent
CSCwb73678	Avertissement de partition /var/tmp remplie sur FXOS
CSCwb74498	Vulnérabilité de l'exécution du code arbitraire et DoS du CDP des logiciels Cisco FXOS et NX-OS
CSCwb82796	Le pare-feu ASA/FTD peut rechercher la source et recharger lors de la destruction des tunnels IKE
CSCwb83691	Recherche de la source et rechargement d'ASA/FTD en raison de la capture initiée à partir du FMC
CSCwb88090	FXOS : Après configuration de FXOS, l'importation d'un nouveau canal de port provoque l'oscillation du canal de port existant
CSCwb90074	ASA : validation de la redirection SFR en mode mixte avec contextes multiples
CSCwb95787	FPR1010 – Aucun ARP sur l'interface VLAN du port du commutateur après l'événement portmanager DIED
CSCwc02133	Vulnérabilité de l'injection de commande des logiciels Cisco FTD et FXOS
CSCwc08683	Voyant DEL de l'interface reste vert et clignote lorsque la fibre optique est débranchée sur le FPR1150

Identifiant	En-tête :
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 »
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
CSCwc27846	Observation d'une panne dans QP(multicontext)-99.18(28)9 pendant la synchronisation à haute disponibilité après la mise à niveau et le rechargement.
CSCwc28806	Recherche de la source et rechargement d'ASA sur le nom de processus Lina
CSCwc31457	Processus ASA avec jeton en texte clair lorsqu'il n'est pas possible de le chiffrer
CSCwc37061	SNMP : FMC ne répond pas à l'OID 1.3.6.1.2.1.25.3.3.1.2
CSCwc38361	Vulnérabilité de l'injection de commande du logiciel Cisco FXOS
CSCwc40352	Lina Netflow envoie des événements autorisés à Stealthwatch, mais ils sont ensuite bloqués par Snort
CSCwc44289	FTD– Recherche de la source et rechargement lors des traductions NAT IPv4 <> IPv6
CSCwc48375	SA IPSEC entrante bloquée inactive – de nombreux SPI entrants pour un SPI sortant dans « show crypto ipsec sa » (afficher crypto ipsec sa)
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
CSCwc61106	Impossible de configurer le domaine\nom d'utilisateur sous cfg-export-policy dans FXOS
CSCwc67687	Le basculement d'ASA HA déclenche l'échec du redémarrage du serveur HTTP et la panne ASDM
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
CSCwc73209	DOC : la clé par défaut est uniquement utilisée par FCM sur FXOS.
CSCwc77519	FPR1120-ASA : le serveur principal joue un rôle actif après le rechargement
CSCwc77680	ASA/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
CSCwc80234	Différence de configuration « inspect snmp » entre actif et veille
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

Identifiant	En-tête :
CSCwc90091	L'ASA 9.12(4)47 avec des statistiques d'utilisateurs affectera la visibilité « policy-server xxxx global ».
CSCwc94466	Vulnérabilité du déni de service SSL/TLS de Cisco ASA/FTD Firepower 2100
CSCwc99242	Port SFP membre du canal ISA 3000 LACP suspendu après le rechargement
CSCwd00778	La sortie ifAdminStatus est anormale via l'interrogation snmp
CSCwd03793	Recherche de la source et rechargement de FTD
CSCwd05756	Recherche de la source FTD sur Lina en raison d'un composant du journal système.
CSCwd22349	ASA : impossible de connecter l'authentification basée sur le certificat AnyConnect avec le « certificat d'authentification périodique » activé
CSCwd31960	L'accès à la gestion sur le VPN ne fonctionne pas lorsque la NAT personnalisée est configurée
CSCwd40260	Amélioration de la convivialité – Impossible d'analyser la charge utile qui est abandonnée en silencieux par ASA/FTD
CSCwd51757	Impossible d'obtenir les résultats de l'interrogation en utilisant snmp GET pour les OID de débit de connexion

Conditions générales de Cisco

Les Conditions générales de Cisco (y compris les autres conditions connexes) régissent l'utilisation des logiciels Cisco. Vous pouvez demande une copie physique à Cisco Systems, Inc., P.O. Box 641387, San Jose, CA 95164-1387. Les logiciels d'autres marques que Cisco achetés auprès de Cisco sont soumis aux conditions de licence applicables du fournisseur. Voir également : https://cisco.com/go/generalterms.

Documentation associée

Pour en savoir plus sur l'ASA, consultez Navigating the Cisco Cisco Secure Firewall ASA Series Documentation (Orientation dans la documentation sur la gamme Cisco).

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.