Correction de l'avis de sécurité SD-WAN de Catalyst - Février 2026

Table des matières

Introduction

Ce document décrit les étapes à suivre pour identifier et corriger les vulnérabilités de sécurité critiques dans SD-WAN en fonction des avis PSIRT datés du 25 février 2026.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Architecture Cisco Catalyst SD-WAN et composants de contrôle (vManage, vSmart, vBond)
- Procédure de mise à niveau SD-WAN de Cisco Catalyst
- Procédures de gestion des dossiers du TAC Cisco et de collecte admin-tech

Composants utilisés

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Pour obtenir des informations détaillées et les dernières mises à jour, reportez-vous à la page d'avis officielle du PSIRT.

Ces conseils sont disponibles à l'adresse suivante :

- Vulnérabilités de Cisco Catalyst SD-WAN
- Vulnérabilité de contournement de l'authentification du contrôleur SD-WAN Cisco Catalyst

Ces défauts sont corrigés par les avis suivants du PSIRT :

- ID de bogue Cisco CSCws52722
- ID de bogue Cisco CSCws33583
- ID de bogue Cisco CSCws33584
- ID de bogue Cisco CSCws33585
- ID de bogue Cisco CSCws33586
- ID de bogue Cisco CSCws33587
- ID de bogue Cisco CSCws93470

Présentation du workflow de résolution

Remarque : Tous les déploiements SD-WAN sont vulnérables et nécessitent une action immédiate. Cependant, tous les systèmes ne présentent pas de signes de compromission.

Action requise : Ouvrez un dossier Cisco TAC pour répondre à cet avis de sécurité.

Le TAC est disponible pour :

- Évaluez votre environnement pour les indicateurs de compromission
- Vous guider tout au long du chemin de correction approprié en fonction de l'évaluation
- Travailler avec l'équipe PSIRT si des indicateurs de compromission sont identifiés
- Fournir une assistance et des conseils de mise à niveau si aucun indicateur de compromission n'est détecté

1. Collecter Admin-Tech - Exécuter admin-tech sur tous les composants de contrôle (vSmart, vManage, vBond). Les admin-techs vSmart ne doivent pas être exécutées simultanément, mais une par une. Tous les autres peuvent être collectés dans n'importe quel ordre. Sélectionnez les options Log et Tech. Core n'est pas requis.
2. Ouvrir le dossier TAC - Contactez le TAC Cisco et fournissez tous les bundles de journaux Admin-tech des composants de contrôle
3. Évaluation du TAC - Le TAC évalue votre environnement pour détecter les indicateurs de compromission
4. Exécuter la correction - Exécutez le processus spécifique fourni par le TAC

Étape 1: Collecter les fichiers Admin-Tech de tous les composants de contrôle

required : Collectez les fichiers admin-tech de tous les composants de contrôle avant d'ouvrir votre dossier TAC. C'est essentiel pour que le TAC puisse évaluer votre environnement.

Collection :

Remarque : Pour la génération admin-tech, sélectionnez les options Log et Tech. Core n'est pas requis.

---

1. Exécutez admin-tech sur TOUS les contrôleurs (vSmarts) - ne les exécutez pas simultanément ; collecter un par un
2. Exécuter admin-tech sur TOUS les managers (vManages)
3. Exécutez admin-tech sur TOUS les validateurs (vBonds)

Remarque : Les admin-techs vSmart ne doivent pas être exécutées simultanément ; collectez-les un par un. Les admin-techs pour les managers et les validateurs peuvent être collectées dans n'importe quel ordre.

Collecte d'un Admin-Tech dans un environnement SD-WAN et téléchargement vers le dossier TAC

Remarque : Le TAC analyse ces fichiers afin d'évaluer votre environnement à la recherche d'indicateurs de compromission et d'orienter le chemin de correction approprié.

Alternative : Vérification manuelle (uniquement si Admin-Tech ne peut pas être

collecté)

Pour ceux qui ne peuvent pas partager de fichiers admin-tech, des étapes de vérification manuelle sont disponibles. Ces étapes fournissent des indicateurs préliminaires qui doivent être documentés et partagés avec le TAC.

Reportez-vous à la section "Étapes de vérification manuelles" à la fin de ce document pour des procédures détaillées. Documentez toutes les conclusions et fournissez-les au TAC dans votre dossier d'assistance.

Étape 2: Ouvrez un dossier TAC et téléchargez les fichiers Admin-Tech

Après avoir collecté tous les fichiers admin-tech de l'étape 1, ouvrez un dossier d'assistance du centre d'assistance technique Cisco.

Actions requises :

1. Ouvrez un dossier TAC avec un niveau de gravité adapté à l'impact sur votre entreprise
2. Téléchargez TOUS les ensembles de journaux admin-tech collectés à l'étape 1 (contrôleurs, gestionnaires et validateurs)
3. Consulter les avis du PSIRT
4. Attendre l'évaluation et les conseils du TAC

⚠ Mise en garde : Le TAC détermine l'état de votre système et recommande les étapes suivantes appropriées.

N'essayez pas d'autres étapes sans conseils du TAC

Étape 3: Évaluation TAC

Le TAC analyse les fichiers admin-tech téléchargés et détermine l'état de votre système.

Pendant cette période :

- Attendez une évaluation officielle du TAC avant de prendre une mesure
- Le TAC vous contacte pour vous faire part de ses conclusions et des prochaines étapes

---

Étape 4: Exécuter la correction (guidé par le TAC)

Le TAC vous guide tout au long du processus de correction approprié en fonction de son

évaluation. Suivez toutes les instructions fournies par le TAC.

Chemin A : Aucun indicateur de compromission trouvé - Mise à niveau

Si le TAC confirme qu'il n'y a aucune preuve de compromission, effectuez une mise à niveau vers la version logicielle fixe. Sélectionnez la version appropriée dans le tableau Versions logicielles fixes de ce document et consultez le guide de mise à niveau lié dans cette section.

Avertissement : La mise à niveau doit rester dans votre version principale actuelle. Ne mettez pas à niveau vers une version majeure supérieure sans conseils explicites du TAC.

Mise à niveau des contrôleurs SD-WAN à l'aide de l'interface utilisateur graphique ou CLI vManage

Chemin B : Indicateurs de compromission identifiés - guidés par le PSIRT

Si le TAC confirme la présence d'indicateurs de compromission, il fait appel à l'équipe PSIRT pour développer une stratégie de correction personnalisée spécifique à votre environnement. Suivez toutes les instructions fournies par le TAC et le PSIRT.

Versions logicielles fixes

Ces versions logicielles contiennent des correctifs pour les vulnérabilités identifiées :

S'applique aux versions actuelles	Version fixe	Logiciels disponibles
20,3, 20,6, 20,9	20.9.8.2 *	Lien disponible 27/02
20.10, 20.11, 20.12.5 et versions antérieures dans 20.12	20.12.5.3	Images de mise à niveau 20.12.5.3 pour vManage, vSmart et vBond
20.12.6	20.12.6.1	Images de mise à niveau 20.12.6.1 pour vManage, vSmart et vBond
20 h 13, 20 h 14, 20 h 15	20.15.4.2	Images de mise à niveau 20.15.4.2 pour vManage, vSmart et vBond
20 h 16, 20 h 17, 20 h 18	20.18.2.1	Images de mise à niveau 20.18.2.1 pour vManage, vSmart et vBond

Remarque : Pour les clients sur CDCS (Cisco-Hosted Cluster), 20.15.405 est également une version fixe. Cela s'applique spécifiquement au déploiement de clusters hébergés par Cisco et est géré séparément du chemin de mise à niveau standard ci-dessus.

* Si vous utilisez la version 20.9 ou une version antérieure : Le logiciel fixe pour votre version (20.9.8.2) est disponible le 27/02. Cisco recommande de rester dans votre version principale actuelle et d'attendre la version 20.9.8.2 plutôt que de mettre à niveau vers une version principale supérieure (20.12, 20.15, 20.18). Si vous utilisez actuellement une version antérieure à 20.9, attendez la mise à niveau de 20.9.8.2. Continuez à travailler avec le centre d'assistance technique et vérifiez le 27/02 pour connaître le lien logiciel disponible.

Références importantes :

- Matrice de mise à niveau
- matrice de compatibilité des contrôleurs

Annexe : Étapes de vérification manuelle (uniquement si la collecte Admin-Tech n'est pas possible)

Remarque : La collecte Admin-tech est la méthode préférée et recommandée. Utilisez uniquement la vérification manuelle si vous ne pouvez absolument pas collecter et partager des fichiers admin-tech. Si vous ne parvenez pas à collecter les fichiers admin-tech, suivez ces étapes manuelles pour collecter les indicateurs préliminaires du TAC.

Remarque :

- Ces étapes fournissent uniquement des données préliminaires
- La collecte admin-tech est vivement recommandée pour une évaluation précise
- Documentez vos conclusions et partagez-les avec le TAC dans votre dossier d'assistance
- Le TAC procède à la détermination officielle de l'évaluation

Exigences: Ces étapes doivent être effectuées sur tous les composants de contrôle.

Vérification 1 : Rechercher les connexions SSH non autorisées dans les journaux d'authentification

Étape 1: Identifier les adresses IP valides du système vManage

Accédez à chaque contrôleur vSmart et exécutez :

```
west-vsmart# show control connections | inc "vmanage|PEER|IP"
```

Exemple de rapport :

```
                                                PEER
      PEER  PEER  PEER            SITE       DOMAIN  PRIV    PEER                                  PUB
INDEX TYPE  PROT  SYSTEM IP       ID         ID      PRIVATE IP                          PORT    PUBLIC I
-------------------------------------------------------------------------------------------------------
0     vmanage dtls 10.1.0.18     101018     0       10.1.10.18                          12346   10.1.10.1
```

Étape 2: Générer une chaîne d'expression régulière (vBond et vSmart uniquement)

Combinez toutes les adresses IP système de l'étape 1 dans un modèle OR regex :

```
system-ip1|system-ip2|...|system-ipn
```

Étape 2b : Étape supplémentaire pour les systèmes vManage

Si vous exécutez ces commandes sur vManage lui-même, ajoutez l'adresse IP localhost (127.0.0.1), l'adresse IP du système local, toutes les adresses IP de cluster et l'adresse IP de l'interface de transport VPN 0 à l'expression régulière :

```
system-ip1|system-ip2|...|system-ipn|127.0.0.1|
```

Pour rechercher l'adresse IP du système vManage local, utilisez :

```
show control local-properties
```

Pour rechercher l'adresse IP de l'interface de transport VPN 0 et l'adresse IP du cluster, utilisez :

```
show interface | tab
```

Étape 3: Exécuter la commande de vérification

Exécutez cette commande, en remplaçant REGEX par votre chaîne regex de l'étape 2 :

```
west-vsmart# vs
west-vsmart:~$ zgrep "Accepted publickey for vmanage-admin from " /var/log/auth.log* | grep -vE "\s(REG
```

Remarque : Cette commande filtre les journaux d'authentification pour afficher uniquement les connexions vmanage-admin provenant de sources inattendues. Les connexions légitimes doivent uniquement provenir des adresses IP associées à vManage.

Étape 4: Interpréter les résultats et le document pour le TAC

Si AUCUN résultat n'est affiché :

- Aucun indicateur de compromission détecté sur ce périphérique
- Documentez ce résultat pour votre dossier TAC
- Poursuivre l'évaluation des contrôleurs restants

Si les lignes du journal sont imprimées :

- Examinez attentivement chaque adresse IP affichée
- Vérifiez que l'adresse IP n'est pas liée à l'infrastructure vManage (adresse IP du cluster, adresse IP de l'ancien système ou similaire)
- Si vous ne pouvez pas identifier l'IP source comme légitime, cela peut indiquer des indicateurs potentiels de compromission
- L'entrée de journal affiche un horodatage et une adresse IP source
- Documenter toutes les conclusions et ouvrir immédiatement un dossier TAC
- Incluez les entrées de journal, les horodatages et les adresses IP source dans votre dossier
- Le TAC procède à la détermination officielle de l'évaluation

Vérification 2 : Rechercher les connexions d'homologue non autorisées dans les syslogs du contrôleur

Cette commande extrait toutes les paires peer-type et peer-system-ip des fichiers syslog du contrôleur et les affiche sous forme de liste que vous pouvez consulter. Il ne signale pas automatiquement les entrées suspectes. Vous devez examiner les résultats et déterminer si chaque adresse IP de système homologue est une partie légitime connue de votre infrastructure SD-WAN. Exécutez cette commande sur tous les composants de contrôle (contrôleurs, gestionnaires et validateurs).

Étape 1: Exécutez la commande sur chaque composant de contrôle :

Tout d'abord, accédez à vshell et accédez au répertoire log :

```
vs
cd /var/log
```

Exécutez ensuite la commande suivante :

```
awk '{
  match($0, /peer-type:([a-zA-Z0-9]+)[^ ]* peer-system-ip:([0-9.:]+)/, arr);
  if(arr[1] && arr[2]) print "(" arr[1] ", " arr[2] ")";
}' vsyslog* | sort | uniq
```

Étape 2: Interpréter les résultats et le document pour le TAC

Si le résultat affiche uniquement les adresses IP connues du système vManage/vSmart/vBond :

- Aucun indicateur de compromission détecté lors de cette vérification
- Documentez ce résultat pour votre dossier TAC
- Poursuivre l'évaluation des autres éléments de contrôle

Si la sortie contient des adresses IP de système homologue non reconnues :

- Examinez attentivement chaque adresse IP et chaque type d'homologue affiché
- Vérifiez que l'adresse IP n'est pas liée à votre infrastructure de plan de contrôle SD-WAN connue
- Si vous ne pouvez pas identifier l'IP source comme légitime, cela peut indiquer des indicateurs potentiels de compromission
- Documenter toutes les conclusions et ouvrir immédiatement un dossier TAC
- Incluez la sortie complète de la commande avec les paires peer-type et peer-system-ip dans votre cas
- Le TAC procède à la détermination officielle de l'évaluation

---

Foire aux questions

Q : Quelle est la première étape pour répondre à cet avis de sécurité ? A : Collectez les fichiers admin-tech de tous les composants de contrôle et ouvrez un dossier TAC pour télécharger les fichiers. Le TAC évalue votre environnement et vous guide dans les étapes suivantes.

Q : Dois-je collecter des admin-techs à partir de tous les composants de contrôle ? A : Oui, le centre d'assistance technique nécessite des fichiers admin-tech de tous les contrôleurs (vSmart, collectés un par un), de tous les gestionnaires (vManage) et de tous les validateurs (vBond) pour

évaluer correctement votre environnement.

Q : Comment le TAC détermine-t-il si mon système a été compromis ? A : Le TAC analyse les fichiers admin-tech à l'aide d'outils spécialisés afin d'évaluer votre environnement et de détecter les indicateurs de compromission.

Q : Que se passe-t-il si des indicateurs de compromission sont identifiés ? A : Le TAC fait appel à l'équipe PSIRT et vous contacte pour discuter des prochaines étapes et des conseils spécifiques à votre environnement. Cisco n'effectue pas la correction en votre nom. Le TAC vous fournit les conseils nécessaires pour poursuivre.

Q : Comment puis-je savoir quelle version de logiciel fixe utiliser ? A : Reportez-vous au tableau Versions logicielles fixes de ce document. Le TAC confirme la version appropriée pour votre environnement spécifique.

Q : Puis-je démarrer la mise à niveau avant que le TAC n'analyse mes admin-techs ? A : Non, attendez que le centre d'assistance technique termine son évaluation et fournisse des conseils avant de tenter des actions correctives.

Q : Un temps d'arrêt est-il attendu pendant la correction ? A : L'impact dépend de votre architecture de déploiement et du chemin de correction. Le TAC fournit des conseils sur la minimisation de l'impact du service pendant le processus.
Q : Les correctifs PSIRT sont-ils inclus dans la prochaine version 20.15.5 et dans d'autres versions à venir ? R : Oui, des correctifs sont inclus dans la version 20.15.5 et dans d'autres versions à venir. Cependant, la mise à niveau visant à atténuer les vulnérabilités décrites dans ce document doit être hiérarchisée IMMÉDIATEMENT. (N'attendez pas !)

Q : Tous les contrôleurs doivent-ils être mis à niveau si aucun indicateur de compromission n'est détecté ? A : Oui, tous les composants de contrôle SD-WAN (vManage, vSmart et vBond) doivent être mis à niveau vers une version logicielle fixe. La mise à niveau d'un seul sous-ensemble de contrôleurs n'est pas suffisante.

Q : J'ai une superposition SD-WAN hébergée dans le cloud. Quelles sont mes options de mise à niveau ? A : Pour les superpositions hébergées dans le cloud, les clients ont deux options :

1. Vérifiez si votre environnement est planifié pour une mise à niveau automatique en accédant à SSP > Overlay Details > Change Windows.
2. Si vous ne souhaitez pas attendre la mise à niveau planifiée, vous avez deux options :
    - Effectuez la mise à niveau par vous-même à l'aide des guides de mise à niveau disponibles dans ce document.
    - Ouvrez un dossier TAC avec la fenêtre de maintenance de votre choix et le TAC vous guide tout au long du processus de mise à niveau.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.