Correction de l'avis de sécurité SD-WAN de Catalyst - Juin 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 4 juin 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 :

- Vulnérabilité de remontée des privilèges authentifiés dans Cisco Catalyst SD-WAN Manager

Ces défauts sont corrigés par les avis suivants du PSIRT :

- ID de bogue Cisco CSCwu18563

Présentation du workflow de résolution

Cet avis décrit une vulnérabilité de remontée des privilèges dans SD-WAN Manager qui nécessite des privilèges d'administrateur réseau pour être exploitée.

Selon l'avis, les chemins connus pour qu'un pirate distant non authentifié obtienne ces privilèges sont l'exploitation de CVE-2026-20182 (cisco-sa-sdwan-rpa2-v69WY2SW) ou de CVE-2026-20127 (cisco-sa-sdwan-rpa-EHchtZk).

Si vos composants de contrôle ont été mis à niveau vers une version fixe pour ces deux avis et que Cisco n'a pas identifié d'indicateurs de compromission (IoC) potentiels dans les fichiers admin-tech que vous avez fournis pour les événements précédents, alors les chemins d'exploitation non authentifiés connus pour cette nouvelle vulnérabilité sont atténués sur ces périphériques spécifiques, en fonction des fichiers examinés.

Cela n'élimine pas l'exposition lorsqu'un pirate détient des informations d'identification netadmin valides. Cisco n'a pas encore publié de correctif logiciel pour cette vulnérabilité et aucune solution de contournement n'est disponible ; d'autres directives suivront dès qu'elles seront disponibles.

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

- Fournir des conseils sur les prochaines étapes à suivre si des indicateurs de compromission sont identifiés

1. Collecter les 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. Ouvrez le dossier TAC- Contactez le TAC Cisco et fournissez tous les bundles de journaux Admin-tech des composants de contrôle.
3. Évaluation du TAC- Effectuez une évaluation préliminaire des indicateurs de compromission dans votre environnement et le TAC effectue une évaluation préliminaire des indicateurs de compromission dans votre environnement.
4. Exécuter la correction - Effectuez le processus spécifique fourni par le TAC si nécessaire.

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 toute mise à niveau ou modification de configuration afin de préserver les données de diagnostic et les indicateurs de compromission (IoC) potentiels. Ces fichiers sont utilisés par le TAC à l'étape 3 pour analyser votre environnement.

Collection : 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)

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 et de détecter les indicateurs de compromission liés à cet avis. L'analyse du présent avis porte sur une entrée de journal spécifique qui ne fait pas de distinction entre l'utilisation légitime et l'utilisation malveillante ; un examen manuel par le TAC est nécessaire.

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

Pour les clients qui ne peuvent pas partager de fichiers admin-tech, une étape de vérification manuelle est disponible. Cette étape fournit un indicateur préliminaire qui doit être documenté et

partagé avec le TAC.

Reportez-vous à la section Étapes de vérification manuelle à la fin de ce document pour la procédure détaillée. 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 les fichiers admin-tech à l'étape 1, ouvrez un dossier d'assistance TAC Cisco et téléchargez les fichiers admin-tech collectés. Le TAC analyse les admin-techs à la recherche d'indicateurs de compromission associés à cet avis.

Actions requises :

1. Ouvrez un dossier TAC de gravité 3 avec « CVE-2026-20245 » et l'ID de conseil `cisco-sa-sdwan-privesc-4uxFrdzx` dans le titre pour lancer l'analyse.
2. Téléchargez TOUS les bundles de journaux admin-tech collectés à l'étape 1 (contrôleurs, gestionnaires et validateurs).
3. Attendez que le TAC termine l'analyse et communique les résultats.

Remarque : Cisco n'a pas publié de correctif logiciel pour cette vulnérabilité et aucune solution de contournement n'est disponible. L'analyse du centre d'assistance technique à l'étape 3 permet de déterminer si des indicateurs de compromission sont présents dans les fichiers admin-tech que vous avez fournis. D'autres conseils suivront dès qu'ils seront disponibles auprès des ingénieurs.

Étape 3: Évaluation TAC

Le TAC effectue une analyse préliminaire des fichiers admin-tech que vous avez téléchargés à l'étape 2 et les évalue pour les indicateurs de compromission associés à cet avis.

Pour cet avis, l'analyse est axée sur une entrée de journal spécifique dans `/var/log/scripts.log` sur chaque gestionnaire (vManage). Étant donné que la commande sous-jacente est légitime et que le journal ne fait pas de distinction entre une utilisation légitime et une utilisation malveillante, toute entrée correspondante doit être examinée manuellement par le TAC par rapport à la position opérationnelle normale du client avant d'être traitée comme un indicateur confirmé.

Résultats possibles de l'analyse du TAC :

- Aucune entrée de journal correspondante n'a été identifiée — d'après les fichiers admin-tech examinés, aucun indicateur associé à cet avis n'a été observé. Aucune autre mesure particulière à cet avis n'est requise pour le moment. Le résultat est limité aux fichiers admin-

tech reçus et peut être limité par la période de rétention du journal sur chaque périphérique.
- Entrées de journal correspondantes identifiées — Le TAC demandera au client de passer en revue les étapes supplémentaires. Comme Cisco n'a pas publié de correctif logiciel pour cet avis, la mise à niveau seule ne résout pas cette vulnérabilité. Les conseils du TAC pour les scénarios de compromission confirmés sont documentés dans les articles TechZone correspondants référencés à l'étape 4.

Remarque : Selon l'avis, l'exploitation de cette vulnérabilité nécessite des privilèges netadmin, qu'un pirate non authentifié ne peut obtenir que par le biais d'informations d'identification valides ou de l'exploitation de CVE-2026-20182 ou CVE-2026-20127. Si vos composants de contrôle ont été mis à niveau vers une version fixe pour ces deux avis et qu'aucun indicateur de compromission n'a été identifié pour les événements précédents, les chemins d'exploitation non authentifiés connus pour cette nouvelle vulnérabilité sont atténués sur ces périphériques spécifiques, en fonction des fichiers examinés.

Étape 4: Si des indicateurs de compromission sont identifiés — Suivez les directives du TAC

Si le TAC identifie des indicateurs de compromission associés à cet avis dans votre environnement, il vous contacte en vous fournissant des conseils spécifiques. Suivez toutes les instructions fournies par le TAC.

Si aucun indicateur de compromission n'est identifié pour cet avis, aucune autre mesure spécifique à cet avis n'est requise pour le moment, d'après les dossiers admin-tech examinés.

Important : Cisco n'a pas publié de correctif logiciel pour cet avis et aucune solution de contournement n'est disponible. Comme l'exploitation de cette vulnérabilité nécessite des privilèges netadmin obtenus par le biais de CVE-2026-20182 ou CVE-2026-20127, les clients doivent s'assurer que la correction de ces avis antérieurs est terminée. Reportez-vous aux documents correspondants pour connaître le flux de conversion établi :

Considérations

À l'issue d'une correction réussie, et en fonction des exigences spécifiques de chaque client en matière d'assurance de la sécurité, les clients peuvent souhaiter évaluer et agir sur les activités d'hygiène suivantes. Ces activités s'appliquent quelle que soit l'option de correction sélectionnée. Ils sont gérés par le client ; Cisco ne les dirige pas et ne les exécute pas pour le compte du client.

- Examen de tous les comptes d'utilisateurs locaux
- Rotation des pouvoirs
- La rotation des secrets présents dans les configurations des périphériques, par exemple (liste non exhaustive) :
    - Informations d'identification des comptes utilisateur locaux
    - Chaînes de communauté SNMP
    - Clés secrètes TACACS
    - Clés et certificats VPN pré-partagés
    - Clés SSH approuvées
- Examen des modèles de configuration

Périphériques de périphérie : compromission suspectée

Cisco ne recommande pas de chemin de résolution particulier ; la sélection d'une option de correction incombe au client. À titre d'information pour les clients évaluant leur environnement : lorsque le client soupçonne la compromission d'un périphérique de périphérie, la réinitialisation et la réintégration en usine du ou des périphériques de périphérie affectés constituent une action gérée par le client que le client peut souhaiter prendre en compte lors de sa sélection. C'est au client qu'il appartient de décider s'il doit poursuivre cette approche et de choisir l'option à sélectionner.

La commande appropriée pour effectuer une réinitialisation d'usine sécurisée est la suivante :

```
factory-reset all secure 3-pass
```

Versions logicielles fixes

⚠ Important : Au moment de la publication de ce document, Cisco n'a pas publié de correctif logiciel pour CVE-2026-20245. Conformément à l'avis, Cisco prévoit de remédier à cette vulnérabilité dans Cisco Catalyst SD-WAN Manager dans une version ultérieure. Il n'y a pas de solution. Cette section sera mise à jour lorsque des logiciels fixes seront disponibles.

Comme l'exploitation de cette vulnérabilité nécessite des privilèges netadmin qu'un attaquant non authentifié ne peut obtenir que par le biais de CVE-2026-20182 ou CVE-2026-20127, les clients sont encouragés à s'assurer que leurs composants de contrôle exécutent une version fixe pour ces avis antérieurs. Les versions corrigées de ces avis sont documentées dans l'avis de sécurité SD-WAN du 14 mai 2026 et dans le document TechZone correspondant :

- Vulnérabilité de contournement de l'authentification du contrôleur SD-WAN Cisco Catalyst (14 mai 2026)

- (Tableau Versions logicielles fixes)

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 privilégiée. Utilisez uniquement l'étape de vérification manuelle ci-dessous si les fichiers admin-tech ne peuvent pas être collectés et partagés avec le TAC. Le résultat de cette étape manuelle est préliminaire ; documenter les résultats et les partager avec le TAC, qui effectue l'évaluation officielle.

Remarque : Pour cet avis, la vérification manuelle consiste en une seule vérification ciblée du journal. L'entrée de journal recherchée est générée par une commande légitime et le journal seul ne fait pas la distinction entre une utilisation légitime et une utilisation malveillante. Toute entrée correspondante doit être comparée à la position opérationnelle normale du client avant d'être traitée comme un indicateur potentiel. Si une entrée correspondante ne peut pas être rapprochée des opérations normales, documentez la conclusion et partagez-la avec le TAC.

Vérification : Vérifiez `scripts.log` sur chaque Manager (vManage) pour les entrées de téléchargement de la liste de locataires

Conformément à l'avis PSIRT, les clients sont encouragés à auditer le fichier `scripts.log`, situé à l'adresse `/var/log/`, pour les entrées similaires à l'exemple suivant :

```
Apr 15 09:44:57 vmanage vScript: Tenant list upload per vsmart serial number: /usr/bin/vconfd_script_up
```

Étape 1: Accédez à vshell sur chaque Manager (vManage) et recherchez le fichier journal

À partir de l'interface de ligne de commande vManage, accédez à vshell et exécutez :

```
vs
zgrep "vconfd_script_upload_tenant_list.sh" /var/log/scripts.log*
```

Répétez la vérification sur chaque vManage du déploiement (y compris tous les membres du cluster et tout vManage associé à un DR).

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

Si AUCUNE entrée correspondante n'est renvoyée :

- Aucun indicateur de compromission associé à cet avis n'a été observé dans le fichier journal de ce périphérique.
- Documentez ce résultat pour votre dossier TAC (indiquez le nom d'hôte du périphérique et la date/plage des fichiers journaux recherchés).
- Poursuivez la vérification sur les gestionnaires restants.

Si des entrées correspondantes sont renvoyées :

- Chaque entrée correspondante doit être comparée à la position opérationnelle normale du client. La commande sous-jacente (téléchargement de la liste de locataires) est légitime et peut apparaître au cours des opérations de routine.
- Pour chaque entrée correspondante, capturez l'horodatage, la ligne de journal complète et le chemin d'accès au fichier référencé après le `chemin d'accès à l'interface de ligne de commande`.
- Si une entrée correspondante ne peut pas être rapprochée d'une opération connue et légitime, cela peut être un indicateur de compromission. Documenter les conclusions et les transmettre au TAC pour examen.
- Documentez toutes les conclusions et ouvrez un dossier TAC. Incluez les entrées de journal correspondantes et le résultat de la commande source dans votre cas.
- Le TAC procède à l'évaluation officielle. Si l'évaluation identifie des indicateurs de compromission, suivez le flux décrit dans les documents TechZone associés : et des guides de correction.

Foire aux questions

Q : Quelle est la première étape pour répondre à cet avis de sécurité ?

A : Collecter les fichiers admin-tech de tous les composants de contrôle (vSmart, vManage, vBond) avant toute mise à niveau ou modification de configuration afin de préserver les données de diagnostic et les indicateurs potentiels de compromission. Ouvrez ensuite un dossier Cisco TAC et téléchargez les admin-techs afin que le TAC puisse les analyser.

Q : Cisco a-t-il publié un correctif logiciel pour cette vulnérabilité ?

A : Pas au moment de la publication de ce document. Conformément à l'avis, Cisco prévoit de remédier à cette vulnérabilité dans Cisco Catalyst SD-WAN Manager dans une prochaine version. Il n'y a pas de solution. Ce document sera mis à jour lorsqu'une version fixe sera disponible.

Q : En l'absence de solution, pourquoi Cisco recommande-t-il une action immédiate ?

A : L'exploitation de cette vulnérabilité nécessite des privilèges netadmin. Conformément à l'avis, un pirate non authentifié peut obtenir ces privilèges uniquement par le biais d'informations d'identification valides ou de l'exploitation de CVE-2026-20182 ou CVE-2026-20127. La mise à niveau des composants de contrôle vers les versions fixes de ces avis précédents permet d'identifier les chemins non authentifiés connus permettant d'obtenir les privilèges requis pour exploiter cette vulnérabilité. L'analyse admin-tech de l'étape 3 permet de déterminer si des indicateurs de compromission sont présents dans les fichiers examinés.

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 effectuer l'analyse.

Q : Comment le TAC détermine-t-il si mon système comporte des indicateurs de compromission associés à cet avis ?

A : Le TAC examine les fichiers admin-tech et recherche l'entrée de journal spécifique décrite dans l'avis PSIRT dans `/var/log/scripts.log` sur chaque manager. La commande sous-jacente est légitime ; toute entrée correspondante doit être comparée à votre position opérationnelle normale avant d'être traitée comme un indicateur potentiel. Le TAC effectue cette révision.

Q : Que se passe-t-il si des indicateurs de compromission sont identifiés ?

A : Le TAC vous contacte pour vous donner des conseils spécifiques. Étant donné qu'aucun correctif logiciel n'est actuellement disponible pour cet avis, la mise à niveau ne résout pas à elle seule une compromission confirmée. Les directives du TAC suivent le flux documenté dans les articles TechZone relatifs aux avis de mai 2026 et de février 2026.

Q : Les routeurs de périphérie (Cisco IOS XE) sont-ils concernés par cet avis ?

A : Cet avis concerne Cisco Catalyst SD-WAN Manager. Conformément à l'avis, Cisco a observé des cas limités où l'exploitation de cette vulnérabilité a entraîné un changement de configuration poussé vers les périphériques de périphérie ; les clients sont invités à vérifier la configuration de leurs périphériques de périphérie.

Q : Quels types de déploiement sont concernés ?

A : Selon l'avis, cette vulnérabilité affecte tous les types de déploiement de Cisco Catalyst SD-WAN Manager, quelle que soit la configuration des périphériques, y compris le déploiement sur site, Cisco SD-WAN Cloud-Pro, Cisco SD-WAN Cloud (géré par Cisco) et Cisco SD-WAN for Government (FedRAMP).

Q : J'ai déjà effectué une mise à niveau pour les avis de mai 2026 et de février 2026 et aucun indicateur de compromission n'a été identifié pour ces événements. Suis-je exposé à cette nouvelle vulnérabilité ?

A : Si vos composants de contrôle exécutent une version fixe pour CVE-2026-20182 et CVE-2026-20127 et qu'aucun indicateur de compromission n'a été identifié pour ces événements

précédents dans les fichiers admin-tech examinés, les chemins d'exploitation non authentifiés connus pour cette nouvelle vulnérabilité sont atténués sur ces périphériques spécifiques, en fonction des fichiers examinés. Cela n'élimine pas l'exposition lorsqu'un pirate détient des identifiants netadmin valides.

Q : Puis-je effectuer la vérification moi-même au lieu d'attendre le TAC ?

A : Les clients qui ne peuvent pas partager admin-techs peuvent effectuer l'étape de vérification manuelle décrite dans l'annexe. Le résultat est préliminaire ; documenter les résultats et les partager avec le TAC, qui effectue l'évaluation officielle.

Q : Quelles sont les meilleures pratiques générales pour renforcer ma superposition SD-WAN ?

A : Reportez-vous au Guide de durcissement SD-WAN de Cisco Catalyst pour connaître les meilleures pratiques.

Q : Le TAC Cisco fournit-il des services d'analyse ou d'investigation pour cette vulnérabilité ?

A : Le TAC Cisco peut aider les clients en examinant les fichiers admin-tech pour les indicateurs de compromission documentés dans l'avis PSIRT. Le TAC de Cisco n'effectue pas d'analyse approfondie ni d'enquête sur les incidents. Pour un travail d'investigation complet ou des enquêtes de sécurité détaillées, les clients sont encouragés à faire appel à leur société de réponse aux incidents (IR) tierce préférée.

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.