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

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

Présentation du workflow de résolution

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

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

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

Étape 3: Évaluation TAC

Étape 4: Si des indicateurs de compromission sont identifiés - Respectez les directives du TAC

Versions logicielles fixes

Considérations

- Périphériques de périphérie : compromission suspectée

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

- Vérification pour CVE-2026-20245 : Vérifiez scripts.log sur chaque composant de contrôle pour les entrées de téléchargement de fichier
- Vérification pour CVE-2026-20262 : Vérifier les entrées d'écriture de fichiers arbitraires dans les fichiers journaux de chaque gestionnaire (vManage)

Foire aux questions

Introduction

Le présent document décrit les étapes à suivre pour identifier et corriger les vulnérabilités de sécurité critiques dans le SD-WAN en fonction des avis émis par le PSIRT les 4 et 15 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 du contrôleur SD-WAN, du gestionnaire SD-WAN et du validateur SD-WAN de Cisco Catalyst
- Vulnérabilité arbitraire d'écriture de fichiers dans Cisco Catalyst SD-WAN Manager

Ces défauts sont corrigés par les avis suivants du PSIRT :

- ID de bogue Cisco CSCwu18563
- ID de bogue Cisco CSCwu18441

Présentation du workflow de résolution

Ces avis décrivent deux vulnérabilités du SD-WAN de Cisco Catalyst. La première (CVE-2026-20245) est une vulnérabilité d'escalade de privilèges dans les composants de contrôle SD-WAN qui nécessite des privilèges d'administrateur réseau pour être exploitée. La deuxième (CVE-2026-20262) est une vulnérabilité d'écriture de fichier arbitraire dans SD-WAN Manager (vManage) qui permet à un utilisateur authentifié de créer ou d'écraser n'importe quel fichier sur le système de fichiers d'un système affecté.

Pour CVE-2026-20245 et CVE-2026-20262, les chemins connus d'un attaquant distant non authentifié pour obtenir les informations d'identification requises sont l'exploitation de CVE-2026-20182 (cisco-sa-sdwan-rpa2-v69WY2SW) ou CVE-2026-20127 (cisco-sa-sdwan-rpa-EHchtZk). CVE-2026-20245 nécessite des privilèges d'administrateur réseau pour l'exploitation, tandis que CVE-2026-20262 nécessite au moins un compte d'utilisateur à tâche unique avec des privilèges inférieurs.

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 CVE-2026-20245 et CVE-2026-20262 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 valides. Cisco vous

recommande d'effectuer une mise à niveau vers une version fixe pour les deux avis.

Action requise : ouvrez un dossier Cisco TAC pour répondre à ces conseils 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 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 - Le TAC effectue une évaluation préliminaire des indicateurs de compromission dans votre environnement en fonction des fichiers admin-tech fournis.
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 un dossier TAC



Remarque : Le TAC analyse ces fichiers afin d'évaluer votre environnement à la recherche d'indicateurs de compromission liés aux deux avis. Pour l'avis d'escalade de privilèges, l'analyse se concentre sur une entrée de journal spécifique dans `/var/log/scripts.log` qui ne fait pas de distinction entre une utilisation légitime et une

---

utilisation malveillante ; un examen manuel par le TAC est nécessaire. Pour l'avis d'écriture de fichier arbitraire, l'analyse se concentre sur les entrées dans `/var/log/nms/vmanage-server.log` ; ces entrées peuvent également se produire pendant les opérations standard et doivent être évaluées par rapport à la position opérationnelle normale pour éviter les faux positifs.

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

Si vous ne pouvez 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 manuelles à la fin de ce document pour une 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 aux deux avis (CVE-2026-20245 et CVE-2026-20262).

Actions requises :

1. Ouvrez un dossier TAC de gravité 3 avec « CVE-2026-20245, CVE-2026-20262 » et les ID de conseil `cisco-sa-sdwan-privesc-4uxFrdzx` et `cisco-sa-sdwan-arbfw-c2rZvQ` 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 a publié des correctifs logiciels pour ces vulnérabilités dans toutes les catégories de versions à l'heure actuelle, mais 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. Effectuez une mise à niveau vers une version logicielle fixe et respectez les directives du TAC concernant toute autre étape suivante nécessaire.

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 aux deux avis (CVE-2026-20245 et CVE-2026-20262).

Pour l'avis CVE-2026-20245, l'analyse se concentre sur une entrée de journal spécifique dans /var/log/scripts.log sur chaque composant de contrôle (vManage, vSmart et vBond). 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 votre position opérationnelle normale avant d'être traitée comme un indicateur confirmé.

Pour l'avis CVE-2026-20262, l'analyse porte sur plusieurs fichiers du répertoire /var/log/nms de chaque manager (vManage). Dans certains cas, ces indicateurs de compromission peuvent se produire lors d'opérations standard.

Ces journaux ne font pas de distinction entre une utilisation légitime et une utilisation malveillante ; par conséquent, toute entrée correspondante doit être examinée manuellement par le TAC par rapport à votre position opérationnelle normale 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 l'un ou l'autre avis n'a été observé. Aucune autre mesure spécifique à ces avis n'est requise pour le moment. Le résultat est limité aux fichiers admin-tech reçus et est soumis à la période de rétention du journal sur chaque périphérique.
- Entrées de journal correspondantes identifiées — Le TAC demande à l'utilisateur de suivre d'autres étapes de révision. Une mise à niveau vers une version fixe est recommandée pour les deux avis. En raison de la nature des avis, des mesures supplémentaires peuvent également être requises. 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 CVE-2026-20245, l'exploitation nécessite des privilèges netadmin, tandis que CVE-2026-20262 nécessite au moins un compte d'utilisateur à tâche unique avec des privilèges inférieurs. Un pirate non authentifié peut obtenir ces informations d'identification 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 conseils et qu'aucun indicateur de compromission n'a été identifié pour les événements précédents, les chemins d'exploitation non authentifiés connus pour CVE-2026-20245 et CVE-2026-20262 sont atténués sur ces périphériques spécifiques, en fonction des fichiers examinés.

Étape 4: Si des indicateurs de compromission sont identifiés - Respectez les directives du TAC

Si le TAC identifie des indicateurs de compromission associés à ces 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 l'un ou l'autre avis, aucune autre action spécifique à l'évaluation de la compromission n'est requise pour le moment, sur la base des fichiers admin-tech examinés. La mise à niveau vers une version fixe pour les deux avis est toujours fortement recommandée.

Versions logicielles fixes

Ces versions logicielles contiennent des correctifs pour les vulnérabilités identifiées :

S'applique aux versions actuelles	Version fixe	Logiciels disponibles
20.9.9.1 et versions antérieures	20.9.9.2	20.9.9.2 images de mise à niveau pour vManage, vSmart et vBond
20.12.7.1 et versions antérieures	20.12.7.2	Images de mise à niveau 20.12.7.2 pour vManage, vSmart et vBond
20.15.4.4 et versions antérieures	20.15.4.5	Images de mise à niveau 20.15.4.5 pour vManage, vSmart et vBond
20.15.5.2 et versions antérieures	20.15.5.3	Images de mise à niveau 20.15.5.3 pour vManage, vSmart et vBond
20.16, 20.17, 20.18.x	20.18.3.1	Images de mise à niveau 20.18.3.1 pour vManage, vSmart et vBond
26.1	26.1.1.2	26.1.1.2 images de mise à niveau pour vManage, vSmart et vBond

---



Remarque : Pour les clients utilisant CDCS (Cisco-Hosted Cluster), 20.15.507 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.

Références importantes :

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

- Correction de l'avis de sécurité SD-WAN de Catalyst — Mai 2026
- Correction de l'avis de sécurité SD-WAN de Catalyst — Février 2026
- Vulnérabilité de contournement de l'authentification du contrôleur SD-WAN Cisco Catalyst (14 mai 2026)

Considérations

À l'issue d'une correction réussie et en fonction de vos exigences spécifiques en matière d'assurance de la sécurité, Cisco vous recommande d'évaluer et de mettre en oeuvre les activités d'hygiène répertoriées ici. Ces activités s'appliquent quelle que soit l'option de correction sélectionnée. Ils sont gérés par l'utilisateur ; Cisco ne les dirige pas et ne les exécute pas en votre nom.

- 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 à chaque client.



Remarque : En cas de suspicion de 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 à prendre en compte lors de votre sélection. C'est à chaque 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
```

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 indiquée ici 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 les deux avis, la vérification manuelle consiste en des vérifications ciblées des journaux. Les entrées de journal ciblées par ces vérifications sont générées par des commandes et des activités légitimes, et les journaux à eux seuls ne font pas la distinction entre une utilisation légitime et malveillante. Toute entrée correspondante doit être comparée à votre position opérationnelle normale 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 pour CVE-2026-20245 : Vérifiez dans **`scripts.log`** sur chaque composant de contrôle les entrées de téléchargement de fichier

Conformément à l'avis du PSIRT, les utilisateurs sont encouragés à vérifier les fichiers journaux à la recherche d'entrées similaires à ces exemples. Dans les versions 20.9 et ultérieures, ces entrées se trouvent dans `scripts.log` à l'adresse `/var/log/`. Sur les versions antérieures à 20.9, les données équivalentes se trouvent dans les journaux `vdebug` à l'adresse `/var/log/tmplog/`.

Trois commandes de téléchargement légitimes distinctes produisent des entrées dans ce même journal avec le même format. Chacun doit être audité :

Exemple d'entrée pour un téléchargement de liste de locataires — `vconfd_script_upload_tenant_list.sh` :

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

Exemple d'entrée pour un téléchargement de numéros de série vSmart — `vconfd_script_upload_vsmart_serial_numbers.sh` :

```
Jun  5 13:06:39 Manager vScript: vSmart upload serial numbers: /usr/bin/vconfd_script_upload_vsmart_ser
```

Exemple d'entrée pour un téléchargement de numéros de châssis ZTP — `vconfd_script_upload_chassis_number_file.sh` :

```
Jun  5 13:08:47 Validator vScript: ZTP upload chassis numbers: /usr/bin/vconfd_script_upload_chassis_nu
```

Étape 1: Accédez à vshell sur chaque composant de contrôle et recherchez les indicateurs CVE-2026-20245 dans les fichiers journaux appropriés

L'emplacement du fichier journal dépend de la version du logiciel exécutée sur le composant de contrôle. Déterminez ce qui s'applique à votre environnement avant d'exécuter la recherche.

Les commandes de recherche ci-dessous utilisent le modèle élargi `vconfd_script_upload_.*\.sh` de sorte qu'un seul appel par emplacement de journal intercepte les trois scripts de téléchargement nommés ci-dessus (`vconfd_script_upload_tenant_list.sh`, `vconfd_script_upload_vsmart_serial_numbers.sh`, et `vconfd_script_upload_chassis_number_file.sh`).

Version 20.9 et ultérieure — Rechercher **`scripts.log`** dans le fichier **`/var/log/tmplog/`** :

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

```
vs
zgrep -E "vconfd_script_upload_.*\.sh" /var/log/scripts.log*
```

Versions antérieures à la version 20.9 — Recherche dans les journaux **`vdebug`** dans **`/var/log/tmplog/`**:

Sur les versions antérieures à 20.9, `scripts.log` n'est pas présent. Les données de journal équivalentes sont écrites dans `/var/log/tmplog/vdebug`. Jusqu'à cinq fichiers numérotés sont conservés (`vdebug`, `vdebug.1` à `vdebug.5`). Rechercher tous les fichiers actifs avec :

```
vs
zgrep -E "vconfd_script_upload_.*\.sh" /var/log/tmplog/vdebug*
```

En plus des fichiers actifs, les journaux plus anciens sont archivés en tant que fichiers tar compressés dans `/var/log/` en utilisant le modèle d'attribution de noms `vdebug_<timestamp>.tar.gz`, avec les données de journal stockées dans l'archive dans `var/log/tmplog`. Rechercher toutes les archives avec :

```
for f in /var/log/vdebug_*.tar.gz; do echo "=== $f ==="; tar -xOf "$f" var/log/tmplog 2>/dev/null | gre
```

Répétez toutes les vérifications applicables sur chaque composant de contrôle dans le déploiement (y compris tous les membres du cluster et tout vManage associé à un routeur désigné).

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 examinée par rapport à votre position opérationnelle normale. Les commandes sous-jacentes (téléchargement de la liste des locataires, téléchargement des numéros de série vSmart et téléchargement des numéros de châssis ZTP) sont légitimes et apparaissent lors 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, il s'agit d'un indicateur potentiel 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, reportez-vous au flux décrit dans les documents TechZone associés : et des guides de correction.

Vérification pour CVE-2026-20262 : Vérifier les entrées d'écriture de fichiers arbitraires dans les fichiers journaux de chaque gestionnaire (vManage)

Conformément à l'avis du PSIRT, les utilisateurs sont encouragés à vérifier ces fichiers journaux sur chaque gestionnaire (vManage) pour les entrées similaires à ces exemples :

Exemple d'entrée suspecte dans `vmanage-server.log` (situé dans `/var/log/nms/`)

```
11-June-2026 03:53:37,310 EDT INFO  [a66cdc5f-807d-4c23-944e-5c809a2ece6b] [server] [SdraAnyConnectFile
```

Exemple d'entrée suspecte dans `vmanage-appserver.log` (situé dans `/var/log/nms/`)

```
11-June-2026 07:52:55,275 UTC INFO  [server] (DeploymentScanner-threads - 2) WFLYSRV0010: Deployed "sus
```

Exemple d'entrée suspecte dans `serviceproxy-access.log` (situé dans `/var/log/nms/containers/service-proxy/`)

```
POST /suspicious/index.jsp HTTP/1.1
```



Remarque : Dans les versions antérieures à la version 20.9, `serviceproxy-access.log` se trouve à l'adresse `/var/log/nms/` plutôt qu'à l'adresse `/var/log/nms/containers/service-proxy/`.

Étape 1: Accédez à vshell sur chaque Manager (vManage) et recherchez les fichiers journaux

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

```
vs
zgrep "SdraAnyConnectFileUploadHandler" /var/log/nms/vmanage-server.log*
zgrep "WFLYSRV0010" /var/log/nms/vmanage-appserver.log*
```

Dans certaines versions, le journal service-proxy est accessible directement depuis vshell. Dans les versions où l'accès au shell racine est requis, téléchargez le admin-tech et recherchez les fichiers `serviceproxy-access.log` dans celui-ci de la même manière en utilisant une commande similaire à :

Versions 20.9 et ultérieures :

```
tar -xOf <admin-tech-filename>.tar.gz var/log/nms/containers/service-proxy/serviceproxy-access.log 2>/d
```

Versions antérieures à la version 20.9 :

```
tar -xOf <admin-tech-filename>.tar.gz var/log/nms/serverproxy-access.log 2>/dev/null | grep "suspicious
```

Si vous accédez directement à partir de vshell, utilisez le nom de fichier .war identifié à partir des

résultats des deux commandes précédentes (sans l'extension) à la place de `suspect` :

Versions 20.9 et ultérieures :

```
zgrep "POST" /var/log/nms/containers/service-proxy/serviceproxy-access.log* | grep "suspicious"
```

Versions antérieures à la version 20.9 :

```
zgrep "POST" /var/log/nms/serverproxy-access.log* | grep "suspicious"
```

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 les fichiers journaux 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 examinée par rapport à votre position opérationnelle normale. Ces entrées peuvent se produire pendant les opérations standard et ne confirment pas la compromission.
- Pour chaque entrée correspondante dans `vmanage-server.log`, capturez l'horodatage, la ligne de journal complète et le chemin d'accès au fichier référencé dans le gestionnaire de téléchargement.
- Si une entrée correspondante ne peut pas être rapprochée d'une opération connue et légitime, il s'agit d'un indicateur potentiel 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, reportez-vous au flux décrit dans les documents TechZone associés : et des guides de correction.

Foire aux questions

Q : Quelle est la première étape pour répondre à ces 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 ces vulnérabilités ?

A : Oui, les versions fixes sont disponibles pour les deux avis, comme indiqué dans la section Versions logicielles fixes. Il n'y a pas de solution.

Q : Pourquoi Cisco recommande-t-il d'agir au-delà de la mise à niveau ?

A : L'exploitation de ces vulnérabilités nécessite un utilisateur authentifié. Un pirate non authentifié ne peut obtenir ces informations d'identification que 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 antérieurs permet d'identifier les chemins non authentifiés connus permettant d'obtenir les privilèges requis pour exploiter ces vulnérabilités. 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 ces avis ?

A : Le TAC examine les fichiers admin-tech pour y trouver des indicateurs de compromission propres à chaque avis. Pour l'avis d'escalade des privilèges (CVE-2026-20245), le TAC recherche des entrées de journal spécifiques dans `/var/log/scripts.log` sur chaque composant de contrôle. Pour l'avis d'écriture de fichier arbitraire (CVE-2026-20262), le TAC recherche des entrées de journal spécifiques dans trois fichiers journaux sur chaque Manager : `/var/log/nms/vmanage-server.log`, `/var/log/nms/vmanage-appserver.log` et `/var/log/nms/containers/service-proxy/serviceproxy-access.log`. Dans les deux cas, l'activité sous-jacente peut avoir lieu au cours d'opérations standard ; toutes les entrées correspondantes sont examinées par le TAC par rapport à votre position opérationnelle normale avant d'être traitées comme un indicateur confirmé.

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

A : Le TAC vous contacte pour vous donner des conseils spécifiques. La mise à niveau seule ne résout pas une compromission confirmée. Les conseils du TAC sont basés sur 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 ces avis ?

A : Ces conseils concernent principalement les composants de contrôle SD-WAN de Cisco Catalyst. Pour l'avis d'escalade des privilèges (CVE-2026-20245), tous les composants de contrôle (vManage, vSmart, vBond) sont affectés, et Cisco a observé des cas limités où l'exploitation a entraîné une modification de configuration poussée vers les périphériques de périphérie ; les utilisateurs sont invités à vérifier la configuration de leurs périphériques de périphérie. Pour l'avis d'écriture de fichier arbitraire (CVE-2026-20262), la vulnérabilité est confinée au système de fichiers du gestionnaire SD-WAN et n'affecte pas directement les périphériques de périphérie.

Q : Quels types de déploiement sont concernés ?

A : Conformément à ces avis, ces vulnérabilités affectent tous les types de déploiement SD-WAN de Cisco Catalyst, quelle que soit la configuration des périphériques, notamment 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 ces nouvelles vulnérabilités ?

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 CVE-2026-20245 et CVE-2026-20262 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 valides. Cisco vous recommande d'effectuer une mise à niveau vers une version fixe pour ces conseils.

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

A : Les utilisateurs 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 ces vulnérabilités ?

A : Le TAC Cisco peut aider les utilisateurs en examinant les fichiers admin-tech pour les indicateurs de compromission documentés dans les deux avis PSIRT. Le TAC de Cisco n'effectue pas d'analyse approfondie ni d'enquête sur les incidents. Pour effectuer un travail d'investigation complet ou des enquêtes de sécurité détaillées, les utilisateurs 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.