# Correction de l'avis de sécurité SD-WAN de Catalyst - Septembre 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 managers

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

Étape 2: Mise à niveau vers une version logicielle fixe

Étape 3: Ouvrez un dossier TAC et téléchargez les fichiers Admin-Tech à analyser

Étape 4: Si une compromission est identifiée — Orientations du TAC

Versions logicielles fixes

- Références importantes

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

- Comment identifier les indicateurs de compromission
- Vérification 1 : Audit du journal d'accès au proxy de service
- Vérification 2 : Audit du journal du serveur Manager

Foire aux questions


## Introduction

Ce document décrit les étapes à suivre pour identifier et corriger une vulnérabilité de sécurité SD-WAN critique conformément aux dates de l'avis PSIRT du 30 septembre 2026. Cisco recommande vivement d'effectuer une mise à niveau vers une version logicielle fixe pour résoudre ce problème.

## Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Architecture et composants de contrôle SD-WAN de Cisco Catalyst (gestionnaire, contrôleur et validateur)
- 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.

Cet avis est disponible sur ce lien :

- Vulnérabilité de contournement de l'authentification de l'API SD-WAN Manager de Cisco Catalyst (CVE-2026-76504, CWE-177). Évaluation de l'impact sur la sécurité : Critique (Score de base CVSS 9.8).

Cette lacune est corrigée par le présent avis du PSIRT :

- ID de bogue Cisco CSCww79570

Cet avis concerne Cisco Catalyst SD-WAN Manager (vManage).

## Présentation du workflow de résolution

---



Remarque : Tous les gestionnaires SD-WAN (vManage) qui exécutent une version antérieure à la première version fixe sont vulnérables et nécessitent une mise à niveau immédiate. Cependant, tous les Catalyst Managers ne présentent pas de signes de compromission.

---

Action requise : Collectez les admin-techs de tous les gestionnaires SD-WAN Catalyst, mettez-les à niveau vers une version fixe et ouvrez un dossier Cisco TAC afin que le TAC puisse analyser vos admin-techs à la recherche d'indicateurs de compromission.

Le TAC est disponible pour :

- Recherchez les indicateurs de compromission dans les techniciens d'administration que vous fournissez
- Fournir une assistance pour la mise à niveau si vous rencontrez des problèmes pendant la mise à niveau
- Vous guider tout au long de la procédure de correction supplémentaire si des indicateurs de compromission sont identifiés

1. Collecter les Admin-Tech - Exécutez admin-tech sur tous les Catalyst SD-WAN Managers, y compris chaque noeud d'un cluster et d'un déploiement de reprise après sinistre (DR), avant la mise à niveau pour garantir qu'aucune donnée de diagnostic n'est perdue. Sélectionnez les options Log et Tech. Core n'est pas requis.
2. Mettre à niveau vers une version fixe - Mettre à niveau tous les gestionnaires (vManage) vers une version fixe répertoriée dans le tableau Versions fixes du logiciel. N'attendez pas les résultats de l'analyse TAC avant de procéder à la mise à niveau. La mise à niveau vers une version fixe est la priorité la plus élevée et permet de supprimer la vulnérabilité. L'analyse TAC de l'étape 3 détermine si d'autres actions sont nécessaires après la mise à niveau.
3. Ouvrez un dossier TAC et téléchargez Admin-Tech pour rechercher les indicateurs de compromission - Ouvrez un dossier TAC Cisco et téléchargez tous les ensembles de journaux admin-tech collectés à l'étape 1. Le TAC recherche les indicateurs de compromission dans les dossiers admin-tech.
4. Si une compromission est identifiée, utilisez les conseils du TAC - Si le TAC identifie des indicateurs de compromission dans votre environnement, suivez tous les conseils de correction fournis par le TAC. Si aucun indicateur de compromission n'est trouvé, aucune action supplémentaire n'est requise au-delà de la mise à niveau.

# Étape 1: Collecter les fichiers Admin-Tech de tous les managers

required : Collectez les fichiers admin-tech de tous les managers (vManage) avant la mise à niveau pour vous assurer qu'aucune donnée de diagnostic n'est perdue. Ces fichiers sont utilisés par le TAC à l'étape 3 pour analyser votre environnement à la recherche d'indicateurs de compromission.

Collection :

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

1. Exécutez admin-tech sur TOUS les managers (vManage).
2. Si vos managers fonctionnent en tant que cluster, exécutez admin-tech sur chaque membre du cluster.
3. Si vous disposez d'un déploiement de reprise après sinistre (DR), exécutez admin-tech sur chaque manager à la fois sur le site principal et sur le site DR.

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

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: Mise à niveau vers une version logicielle fixe

Après avoir collecté les admin-techs à l'étape 1, mettez à niveau tous les managers (vManage) vers une version logicielle fixe.

⚠ Important : N'attendez pas les résultats de l'analyse TAC avant de procéder à la mise à niveau. La mise à niveau vers une version fixe est la priorité la plus élevée et permet de supprimer la vulnérabilité. L'analyse TAC de l'étape 3 détermine si d'autres actions sont nécessaires après la mise à niveau.

Sélectionnez la version appropriée dans le tableau Versions logicielles fixes de ce document.

⚠ 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

Si vous rencontrez des problèmes lors de la mise à niveau, ouvrez un dossier TAC pour obtenir de l'aide sur la mise à niveau.

## Étape 3: Ouvrez un dossier TAC et téléchargez les fichiers Admin-Tech à analyser

Après la mise à niveau de l'étape 2, ouvrez un dossier d'assistance du TAC Cisco et téléchargez les fichiers admin-tech collectés à l'étape 1. Le TAC recherche les indicateurs de compromission sur les techniciens admin.

Actions requises :

1. Ouvrez un dossier TAC de gravité 3 avec l'ID CVE "CVE-2026-76504" dans le titre pour lancer le processus de numérisation.
2. Téléchargez TOUS les ensembles de journaux admin-tech collectés à l'étape 1 (tous les gestionnaires, y compris les noeuds de cluster et de reprise après sinistre).

3. Attendez que le TAC termine l'analyse et communique les résultats.

Le TAC analyse les fichiers admin-tech et communique les résultats de l'analyse. Si aucun indicateur de compromission n'est trouvé, aucune action supplémentaire n'est requise au-delà de la mise à niveau.

## Étape 4: Si une compromission est identifiée — Orientations du TAC

Si le TAC identifie des indicateurs de compromission dans votre environnement, il vous contacte pour vous fournir des conseils de correction spécifiques. Suivez toutes les instructions fournies par le TAC.

Si aucun indicateur de compromission n'est identifié, la mise à niveau effectuée à l'étape 2 est suffisante et aucune autre correction n'est requise.

## Versions logicielles fixes

Ces versions logicielles contiennent le correctif pour cette vulnérabilité. Effectuez une mise à niveau vers la première version fixe de votre catégorie de version actuelle.

| Version du logiciel Cisco Catalyst SD-WAN | Première Version Fixe | Logiciels disponibles |
|---|---|---|
| Antérieure à 20.9[1] | Migrer vers une version fixe. | |
| 20.9 | 20.9.10.1 | Images de mise à niveau 20.9.10.1 pour vManage |
| 20.12 | 20.12.8.2 | Images de mise à niveau 20.12.8.2 pour vManage |
| 20.15 | 20.15.6.1 | Images de mise à niveau 20.15.6.1 pour vManage |
| 20.18 | 20.18.4.1 | Images de mise à niveau 20.18.4.1 pour vManage |
| 26.1 | 26.1.2.1 | Images de mise à niveau 26.1.2.1 pour vManage |
| 26.2 | 26.2.1 | Images de mise à niveau 26.2.1 pour vManage |

[1] Ces versions ont atteint la fin de la maintenance logicielle. Cisco encourage vivement les clients à passer à une version prise en charge.

L'équipe PSIRT (Product Security Incident Response Team) de Cisco valide uniquement les informations relatives aux versions affectées et fixes documentées dans l'avis.

Cisco a également remédié à cette vulnérabilité dans la version 20.15.605 de Cisco SD-WAN

Cloud (Cisco Managed), basée sur le cloud. Aucune action de l'utilisateur n'est requise. Les clients peuvent déterminer l'état de correction actuel ou la version du logiciel à l'aide de la fonction Aide de l'interface utilisateur graphique du service.

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)

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.

- 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 gestionnaires (vManage), y compris chaque membre du cluster et chaque gestionnaire d'un site de reprise après sinistre (DR). Accédez aux fichiers journaux à partir de vshell (vshell à partir de l'interface de ligne de commande de Manager) et examinez les fichiers journaux actuels et les fichiers journaux pivotés.

## Comment identifier les indicateurs de compromission

Cet avis comporte deux indicateurs de compromission. Les deux concernent des entrées pour j_security_check dans lesquelles un caractère de la requête est codé (par exemple /%6a_security_check), à partir d'adresses IP inconnues ou non autorisées.

---

⚠ Important : Les exemples de cette section montrent l'utilisation de %6a comme caractère codé j dans la requête. Ce n'est qu'un exemple, et la vulnérabilité permet d'utiliser n'importe quel caractère codé dans la requête.

---

Les systèmes Cisco Catalyst SD-WAN Manager exposés à Internet et dont les ports sont exposés à Internet risquent d'être compromis. Dans certains cas, ces indicateurs de compromission peuvent se produire lors d'opérations standard. Par conséquent, ils doivent être évalués par rapport à la position normale du réseau pour identifier et éviter les faux positifs.

| Indicateur | Fichier journal | Ce que cela signifie | Vérification |
|---|---|---|---|
| Demande j_security_check codée reçue | /var/log/nms/containers/service_proxy/serviceproxy-access.log* | Un client a envoyé une demande de ce type au responsable. | Vérification 1 |
| Demande j_security_check codée traitée pour un utilisateur viptela-reserved-* | /var/log/nms/vmanage-server.log* | Le gestionnaire a traité une demande de ce type pour un utilisateur viptela-reserved-* (un compte de service système réservé). | Vérification 2 |

## Vérification 1 : Audit du journal d'accès au proxy de service

Vérifiez dans le fichier serviceproxy-access.log, situé à l'adresse /var/log/nms/containers/service_proxy/serviceproxy-access.log, les entrées liées à j_security_check provenant d'adresses IP inconnues ou non autorisées, comme indiqué dans cet exemple :

```
[2026-09-29T23:11:13.948-05:00] "POST /%6a_security_check HTTP/1.1" 200 - 48 0 4 - "10.10.10.47,192.168
```

Certains fichiers journaux du système vManage sont restreints derrière l'accès racine et ne sont pas accessibles directement par les clients. Pour consulter ces journaux, les clients doivent générer un fichier admin-tech.

Interpréter les résultats et le document pour le TAC

Si aucune entrée de ce type n'est trouvée :

- Aucun indicateur de compromission détecté dans ce journal sur ce gestionnaire
- Documentez ce résultat pour votre dossier TAC
- Passez à la vérification 2, puis répétez les deux vérifications sur les gestionnaires restants

Si de telles entrées sont trouvées :

- Examinez attentivement chaque adresse IP source affichée
- Recherchez les entrées provenant d'adresses IP inconnues ou non autorisées. Vérifiez si l'adresse IP source appartient à une activité autorisée dans votre environnement (par

exemple, une analyse de vulnérabilité ou un test de pénétration que vous exécutez)
- 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 les entrées de journal, les horodatages, les adresses IP source et les codes d'état HTTP dans votre cas
- Le TAC procède à la détermination officielle de l'évaluation

### Vérification 2 : Audit du journal du serveur Manager

Vérifiez dans le fichier vmanage-server.log, situé à l'adresse /var/log/nms/vmanage-server.log, les entrées liées à j_security_check provenant d'adresses IP inconnues ou non autorisées, en particulier lorsqu'elles sont appelées pour des utilisateurs dont les noms commencent par viptela-reserved-, comme indiqué ici :

```
29-Sep-2026 23:11:13,952 CDT [] [vManage-new] [UserUtils] (default task-127462) |default| Request Store
```

Les comptes de service système réservés à viptela sont documentés dans la section Authentication, Authorization, and Accounting du Guide de configuration des interfaces et systèmes SD-WAN de Cisco Catalyst.

Interpréter les résultats et le document pour le TAC

Si aucune entrée de ce type n'est trouvée :

- Aucun indicateur de compromission détecté dans ce journal sur ce gestionnaire
- Documentez ce résultat pour votre dossier TAC
- Répétez les deux vérifications sur les managers restants

Si de telles entrées sont trouvées :

- Cela peut indiquer des indicateurs potentiels de compromission
- Documenter toutes les conclusions et ouvrir immédiatement un dossier TAC
- Incluez les entrées de journal et les horodatages de votre dossier, ainsi que les résultats de la vérification 1 pour la même période
- Le TAC procède à la détermination officielle de l'évaluation

## Foire aux questions

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

Collectez les fichiers admin-tech de tous les managers (vManage), puis mettez à niveau tous les managers vers une version logicielle fixe. Après la mise à niveau, ouvrez un dossier TAC et téléchargez les admin-techs afin que le TAC puisse analyser votre environnement à la recherche d'indicateurs de compromission.

Quels composants sont concernés par cet avis ?

Seul Cisco Catalyst SD-WAN Manager (vManage) est concerné.

Devons-nous également mettre à niveau les contrôleurs, les validateurs ou les routeurs de périphérie ?

Non, pas pour répondre à cet avis. Mettez à niveau tous les gestionnaires (vManage) vers une version fixe et utilisez la matrice de compatibilité des contrôleurs pour confirmer que la nouvelle version de Manager est compatible avec vos autres composants.

Une solution de contournement est-elle disponible ?

Non. Il n'existe aucune solution de contournement pour résoudre cette vulnérabilité. Effectuez une mise à niveau vers une version fixe.

Quelle version dois-je mettre à niveau ?

Effectuez une mise à niveau vers la première version fixe de votre version actuelle dès que possible. Reportez-vous au tableau Versions logicielles fixes de ce document. Le TAC confirme la version appropriée pour votre environnement spécifique.

J'ai déjà effectué une mise à niveau vers une version fixe pour un avis de sécurité SD-WAN précédent. Dois-je effectuer une nouvelle mise à niveau ?

Oui, sauf si votre version actuelle est antérieure ou égale à la première version fixe de votre catégorie dans le tableau Versions logicielles fixes. Les versions corrigées pour les avis antérieurs n'incluent pas nécessairement le correctif pour cette vulnérabilité.

Dois-je collecter des admin-techs auprès de tous les managers ?

Oui. Le centre d'assistance technique (TAC) a besoin des fichiers admin-tech de chaque gestionnaire (vManage), y compris chaque membre du cluster et chaque gestionnaire d'un site de reprise après sinistre (DR), pour évaluer correctement votre environnement.

Puis-je vérifier moi-même les indicateurs de compromission ?

Oui. Si vous ne pouvez pas collecter de fichiers admin-tech, utilisez les étapes de vérification manuelles sur chaque manager et partagez les résultats avec le TAC. La collecte admin-tech reste la méthode privilégiée, et le TAC procède à la détermination officielle de l'évaluation.

Comment le TAC détermine-t-il si mon système a été compromis ?

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.

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

Le TAC 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.

Puis-je démarrer la mise à niveau avant que le TAC n'analyse mes admin-techs ?

Oui. Collectez les admin-techs, effectuez une mise à niveau vers une version fixe, puis ouvrez un dossier TAC afin que le TAC puisse analyser les admin-techs à la recherche d'indicateurs de compromission.

Un temps d'arrêt est-il attendu pendant la correction ?

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.

J'ai une superposition SD-WAN hébergée dans le cloud. Quelles sont mes options de mise à niveau ?

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 de secours pour votre fenêtre de maintenance préférée. Le centre d'assistance technique est à votre disposition si vous rencontrez des difficultés avec la mise à niveau.

Nous sommes une superposition hébergée par Cisco. Devons-nous revoir les règles d'accès sur le SSP ?

Tous les clients hébergés par Cisco sont invités à consulter leurs propres règles entrantes autorisées dans SSP > Overlay Details > Allow Inbound rules et à s'assurer que seuls les préfixes nécessaires de votre côté sont autorisés. Ces règles sont uniquement destinées à l'accès à la gestion et ne s'appliquent pas aux routeurs de périphérie.

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

Le centre d'assistance technique Cisco peut aider les clients en recherchant des indicateurs de compromission (IoC) associés à cette vulnérabilité. Toutefois, le TAC ne procède pas à une analyse approfondie des enquêtes judiciaires ou des incidents. Pour un travail d'investigation complet ou des enquêtes de sécurité détaillées, nous recommandons aux clients de faire appel à leur société de réponse aux incidents (IR) tierce préférée.

Quelles sont les meilleures pratiques générales ou les moyens de réduire les vulnérabilités de ma superposition SD-WAN ?

Reportez-vous au Guide de durcissement SD-WAN de Cisco Catalyst pour connaître les meilleures pratiques et les recommandations visant à réduire les vulnérabilités dans votre superposition SD-WAN.

Quelles versions du contrôleur (vSmart) et du validateur (vBond) dois-je exécuter avec la version du gestionnaire (vManage) qui corrige cet avis ?

Cet avis concerne uniquement Cisco Catalyst SD-WAN Manager (vManage). Par conséquent, seul le Manager passe à une nouvelle version. Mettez à niveau chaque manager vers la première version fixe de votre train dans le tableau Versions logicielles fixes.

Les contrôleurs et les validateurs n'ont pas besoin d'une mise à niveau pour cet avis : ils sont censés exécuter déjà la version fixe publiée dans la version de sécurisation renforcée du logiciel Cisco Catalyst SD-WAN : Août 2026, et cette version dans le même train est le jumelage attendu pour la version fixe de Manager.

Votre catégorie de versions est la famille de versions principale que vous exécutez aujourd'hui, par exemple 20.9, 20.12, 20.15, 20.18, 26.1 ou 26.2. La première version fixe est la version la plus ancienne de cette catégorie qui contient le correctif, et c'est le chemin le plus court et le moins risqué vers la correction, car vous restez dans la catégorie que vous exécutez déjà. Il n'est pas nécessaire de passer à un train plus récent pour donner suite à cet avis. Si votre manager est déjà à la première version fixe de votre train ou plus tard, il n'est pas affecté et aucune mise à niveau n'est requise. Seules les versions antérieures à la version 20.9 nécessitent une migration vers une catégorie prise en charge, car ces versions ont atteint la fin de la maintenance logicielle.

Utilisez votre processus de mise à niveau normal et le même accélérateur de maintenance que celui utilisé pour l'avis précédent. La seule modification consiste à sélectionner la nouvelle image du manager. Par exemple, dans le train 20.15 :

- Manager (vManage) - 20.15.6.1
- Contrôleurs (vSmart) et validateurs (vBond) — 20.15.6

Si vos composants de contrôle sont toujours sur une version antérieure à l'avis d'août 2026, suivez l'ordre de mise à niveau SD-WAN standard et commencez par le gestionnaire. Par exemple, si vos composants sont sur 20.9.5 :

1. Mettez à niveau chaque Manager (vManage) directement vers la version qui corrige cet avis, qui est 20.9.10.1 dans la catégorie 20.9.
2. Mettez à niveau les validateurs (vBond) et les contrôleurs (vSmart) vers la version fixe d'août 2026 pour ce train, à savoir 20.9.10.

Dans cet exemple, l'état final est Managers à 20.9.10.1 et Validators et Controllers à 20.9.10. Les versions 20.9 ne sont présentées qu'à titre d'exemple ; appliquez la même séquence au train que vous exécutez, en utilisant le tableau Versions logicielles fixes pour identifier la version de Manager correcte pour votre train.

Où puis-je vérifier quelles versions de Controller (vSmart) et Validator (vBond) sont compatibles avec la version de Manager (vManage) qui contient ce correctif ?

Utilisez la matrice de compatibilité des contrôleurs. Recherchez la version Manager vers laquelle vous effectuez la mise à niveau dans le tableau Versions logicielles fixes et confirmez les versions de contrôleur et de validateur prises en charge. La Matrice de mise à niveau indique les chemins

de mise à niveau pris en charge pour atteindre cette version.

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.