Correction de l'avis de sécurité SD-WAN de Catalyst - Mai 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: 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 un problème est identifié, suivez les instructions du TAC

Versions logicielles fixes

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

- Vérification 1 : Rechercher les connexions SSH non autorisées dans les journaux d'authentification
- Vérification 2 : Rechercher les connexions d'homologue non autorisées dans les syslogs du contrôleur
- Vérification 3 : Vérifier si une demande de confirmation est manquante sur les connexions de contrôle actif

Foire aux questions

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

Ces défauts sont corrigés par les avis suivants du PSIRT :

- ID de bogue Cisco CSCwt50498
- ID de bogue Cisco CSCwt38739
- ID de bogue Cisco CSCwt38767
- ID de bogue Cisco CSCwt55544

Présentation du workflow de résolution



Remarque : Tous les contrôleurs et gestionnaires SD-WAN sont vulnérables et nécessitent une mise à niveau immédiate pour tous les composants de contrôle. Cependant, tous les contrôleurs ne montrent pas de signes de compromission.

Action requise : Collectez les admin-techs, effectuez une mise à niveau vers une version fixe, puis 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 Admin-Tech - Exécutez admin-tech sur tous les composants de contrôle (vSmart, vManage, vBond) avant la mise à niveau pour vous assurer qu'aucune donnée de diagnostic

n'est perdue. Sélectionnez les options Log et Tech. Core n'est pas requis.



Mise en garde : 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

2. Mise à niveau vers une version fixe - Mettez à niveau tous les composants de contrôle SD-WAN (vManage, vSmart, vBond) vers une version logicielle fixe répertoriée dans le tableau Versions logicielles fixes.



Remarque : 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, suivez 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 composants de contrôle

required : Collectez les fichiers admin-tech de tous les composants de contrôle 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 :



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: Mise à niveau vers une version logicielle fixe

Après avoir collecté les admin-techs à l'étape 1, mettez à niveau tous les composants de contrôle SD-WAN (vManage, vSmart et vBond) 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]

Remarque : 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 « CVE-2026-20182 » et l'ID PSIRT approprié dans le titre pour lancer le processus de numérisation.
2. Téléchargez TOUS les ensembles 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 : 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 un problème est identifié, suivez les instructions 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 des correctifs pour les vulnérabilités identifiées :

Avertissement : Bien que nous recommandions de suivre les conseils du tableau, il est essentiel que les clients choisissant de mettre à niveau de 20.9.x vers 20.12.x déploient la version 20.12.7.1 pour éviter de rencontrer le bogue Cisco ayant l'ID CSCwm9530.

S'applique aux versions actuelles	Version fixe	Logiciels disponibles
20,3, 20,6, 20,9	20.9.9.1	Images de mise à niveau 20.9.9.1 pour vManage, vSmart et vBond
20.10, 20.11, 20.12.5 et versions antérieures dans 20.12	20.12.5.4	Images de mise à niveau 20.12.5.4 pour vManage, vSmart et vBond
20.12.6.x	20.12.6.2	Images de mise à niveau 20.12.6.2 pour vManage, vSmart et vBond
20.12.7	20.12.7.1	Images de mise à niveau 20.12.7.1 pour vManage, vSmart et vBond
20.13, 20.14, 20.15.4.3 et versions antérieures dans 20.15	20.15.4.4	Images de mise à niveau 20.15.4.4 pour vManage, vSmart et vBond
20.15.5.x	20.15.5.2	Images de mise à niveau 20.15.5.2 pour vManage, vSmart et vBond
20.16, 20.17, 20.18.x	20.18.2.2	Images de mise à niveau 20.18.2.2 pour vManage, vSmart et vBond

Remarque : pour les clients utilisant le cloud SD-WAN (anciennement appelé Cloud Delivered Cisco Catalyst SD-WAN [CDCS]), la version 20.15.506 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. Tous ces clients sont déjà mis à niveau vers la version fixe 20.15.506.

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 this pour rechercher le glob du fichier vsyslog* :

```
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
```

Répétez cette procédure pour messages* file glob ainsi que vdebug* file glob.

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

Vérification 3 : Vérifier si une demande de confirmation est manquante sur les connexions de contrôle actif

Cette vérification examine la sortie du détail des connexions de contrôle pour les sessions homologues qui sont signalées comme actives (ou récemment désactivées) mais qui manquent l'échange de `confirmation` attendu. Une session qui échange des paquets `hello` dans les deux directions tout en affichant `challenge-ack 0` dans les statistiques Tx ou Rx indique que l'homologue n'a jamais terminé la connexion de défi attendue — une anomalie qui justifie une enquête. Exécutez cette commande sur tous les composants de contrôle (contrôleurs, gestionnaires et validateurs).

Étape 1: Collecter le résultat détaillé des connexions de contrôle

À partir de la CLI du périphérique, exécutez :

```
show control connections detail
show control connections-history detail
```

Enregistrez le résultat dans un fichier (par exemple, `vdaemon.txt`) pour inspection.

Étape 2: Que faut-il rechercher ?

Pour chaque enregistrement homologue (délimité par les en-têtes `REMOTE-COLOR-` / `SYSTEM-IP-`), marquez l'enregistrement si toutes les conditions suivantes sont vraies :

- L'état de la session est UP ou TEAR_DOWN
- Les compteurs Hello Tx Statistics et Rx Statistics sont tous deux non nuls (les paquets Hello circulent dans les deux directions)
- challenge-ack est 0 dans le bloc Tx Statistics et Rx Statistics

Exemple d'enregistrement correspondant (notez les flèches `<<<` mettant en évidence le `challenge-ack` manquant)

```
------------------------------------------------------------------------------------------
 REMOTE-COLOR- default SYSTEM-IP- 10.2.2.2   PEER-PERSONALITY- vmanage
------------------------------------------------------------------------------------------
site-id             432567
domain-id           0
protocol            dtls
private-ip          10.0.0.1
private-port        12346
public-ip           192.168.1.1
public-port         50825
state               up [Local Err: NO_ERROR] [Remote Err: NO_ERROR]
uptime              0:00:16:58
hello interval      1000
hello tolerance     12000

  Tx Statistics-
  --------------
    hello                   3423293
    challenge               1
    challenge-response      0
    challenge-ack           0           <<<< MISSING challenge-ack (Tx)
    ...

  Rx Statistics-
  --------------
    hello                   3423291
    challenge               0
    challenge-response      1
    challenge-ack           0           <<<< MISSING challenge-ack (Rx)
    ...
```

Dans l'exemple ci-dessus, les compteurs `Hello` Tx et Rx sont non nuls (connexion active), mais le `challenge-ack` est `0` dans les deux directions.

Étape 3: Commande Recherche manuelle

Pour afficher rapidement les enregistrements candidats d'un fichier `vdaemon.txt` enregistré (ou de tout fichier contenant la sortie `show control connections detail`), exécutez :

```
grep -A20 'SYSTEM-IP' vdaemon.txt | grep -B5 'challenge-ack  0'
```

Chaque bloc renvoyé représente une session homologue où la demande de confirmation est signalée comme 0. Vérifiez chaque bloc dans son intégralité pour confirmer que l'état est `up` ou `tear_down` et que les compteurs d'`HELLO` dans Tx et Rx sont non nuls avant de le traiter comme un résultat.

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

Si aucun enregistrement ne remplit les trois conditions :

- 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 un ou plusieurs enregistrements remplissent les trois conditions :

- Examinez attentivement les valeurs `SYSTEM-IP-`, `private-ip` et `public-ip` pour chaque enregistrement marqué
- Vérifiez que l'homologue n'est pas une partie légitime connue de votre plan de contrôle SD-WAN (membre du cluster, site de reprise après sinistre, adresse IP précédemment attribuée à un composant)
- Si vous ne pouvez pas identifier l'homologue comme légitime, cela peut indiquer des indicateurs potentiels de compromission
- Documenter toutes les conclusions et ouvrir immédiatement un dossier TAC
- Inclure le ou les enregistrements homologues correspondants complets et le résultat de la commande source dans votre dossier
- 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, puis mettez à niveau tous les composants de contrôle 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.

Q. Quelle version dois-je utiliser pour effectuer la mise à niveau ?

R. Veuillez effectuer la mise à niveau vers la version fixe la plus proche au plus tôt.

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 : Existe-t-il un moyen d'effectuer ma propre analyse automatisée à l'aide des outils du TAC ?

A : Les clients peuvent également utiliser l'outil en libre-service « Vérifier l'applicabilité du bogue »

qui est intégré à la page Outil de recherche de bogue pour l'ID de bogue Cisco CSCwt50498 pour analyser à nouveau admin-techs à partir des composants de contrôle.

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

A : 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.

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 : 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.

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 : 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 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.

Q : Devons-nous également mettre à niveau les routeurs de périphérie ?

A : Non, les périphériques Cisco IOS XE ne sont pas concernés par cet avis.

Q : Nous sommes une superposition hébergée par Cisco. Devons-nous corriger des listes de contrôle d'accès ou prendre des mesures sur SSP ?

A : Il est conseillé à tous les clients hébergés par Cisco de consulter leurs propres règles de trafic entrant autorisé sur SSP et de s'assurer que seuls les préfixes nécessaires de votre côté sont autorisés. Ces règles concernent uniquement l'accès à la gestion et ne s'appliquent pas aux routeurs de périphérie. Vérifiez-les dans SSP > Overlay Details > Allow Inbound rules. Notez que le port 22 et 830 étaient toujours bloqués par défaut lors de la mise en service du jour 0 par Cisco de l'extérieur vers les contrôleurs hébergés dans le cloud.

Q : Nous utilisons le cloud SD-WAN (anciennement appelé CDCS (Cloud Delivered Cisco Catalyst SD-WAN)). Quelle version allons-nous mettre à niveau ?

A : D'après la version actuelle, les clusters de cloud SD-WAN sont actuellement planifiés pour être mis à niveau OU ont déjà été mis à niveau vers les versions fixes. Voici les versions fixes du cloud SD-WAN (anciennement CDCS) :

1. Clusters d'adoption précoce = 20.18.2.2 (il s'agit en fait de la même version que la version standard)

2. Recommandations de clusters de version = 20.15.506 (version CDCS spécifique avec correctifs PSIRT)

Les clients du cloud SD-WAN n'ont pas besoin de prendre des mesures efficaces pour répondre à ce PSIRT.

Q : Nous sommes sur le service partagé. Quelle version allons-nous mettre à niveau ?

A : En fonction de la version actuelle, le service partagé partagé est actuellement planifié pour être mis à niveau OU déjà mis à niveau vers les versions fixes. Voici les versions fixes du service partagé :

1. Recommandations de clusters de version = 20.15.5.2

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

A : Le centre d'assistance technique Cisco peut aider les clients en recherchant des indicateurs de compromission (IoC) associés à ces vulnérabilités. 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.

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

A : 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.

Q : Nous voyons les journaux d'un utilisateur « root » sur notre système. Est-ce inquiétant ?

A : Vérifiez ce qui se passe d'autre dans le système à ce moment-là. Ces journaux sont tout à fait prévisibles. Par exemple, les journaux system-login-change d'un utilisateur « root » sont visibles lorsque les admin-techs sont générées. Les journaux peuvent également être vus par un utilisateur « racine » lors d'un redémarrage.

```
Feb 28 23:03:44 Manager01 SYSMGR[863]: %Viptela-Manager01-sysmgrd-6-INFO-1400002: Notification: system-

       user-name:"root" user-id:245  generated-at:2-28-2026T23:3:44

Feb 28 23:03:47 Manager01 SYSMGR[863]: %Viptela-Manager01-sysmgrd-6-INFO-1400002: Notification: system-

        user-name:"root" user-id:248  generated-at:2-28-2026T23:3:47
```

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.