

Rechercher les articles existants en gras

Table des matières

[Introduction](#)

[Références — Documentation Cisco SD-WAN CVE-2026-20182](#)

[E-mails](#)

[Sherlock 1 - Admission - Demande de mise à niveau et fichiers Admin-Tech](#)

[Sherlock 2 - Résultat - Aucune IoC observée \(par fichier\)](#)

[Sherlock 3 - Rappel - Fichiers Admin-Tech manquants](#)

[TAC 1 - Enquête - Examen supplémentaire requis \(IoC suspecté\)](#)

[TAC 2 - Résultat - Aucun IoC trouvé \(confirmé par l'ingénieur\)](#)

[TAC 3 - Validation - Confirmer la propriété IP dans la superposition](#)

[TAC 4 - Résultat - Faux positif effacé](#)

[TAC 5 - Critique - Identification de l'IoC, appel de révision du calendrier](#)

[TAC 6 - Résultat - IoC en double \(Fermer et rediriger\)](#)

[TAC 7 - Correction - Suivi des options \(post-appel\)](#)

[TAC 8 - Correction - Options mises à jour pour les fabricants compromis \(suivi de l'option 2\)](#)

[TAC 17 - Constatation inversée : auparavant, aucune IoC, maintenant identifiée \(CVE-2026-20182\)](#)

[CloudOps 1 - Proactive - IoC détecté dans l'analyse du cloud, Admin-Tech requis pour la validation](#)

[E-mails pour la VAGUE 2A pour les clients PRÉCÉDEMMENT CONCERNÉS qui n'ont pas déjà complété les options A, B ou C. \(Les options 1 et 2 doivent être refaites\)](#)

[Modèle TAC 9 pour aucun CIO pour PSIRT2a/ils ont reconstruit \(PRÉCÉDEMMENT IMPACTÉ\)](#)

[Modèle TAC 10 pour oui IOC pour PSIRT2a/ils ont reconstruit \(PRÉCÉDEMMENT IMPACTÉ\)](#)

[Modèle TAC 11 pour aucun CIO pour PSIRT2a/ils n'ont pas reconstruit \(PRÉCÉDEMMENT TOUCHÉ\)](#)

[Modèle TAC 12 pour oui COI pour PSIRT2a/ils n'ont pas reconstruit \(PRÉCÉDEMMENT IMPACTÉ\)](#)

[E-mails pour la VAGUE 2A pour les NOUVEAUX clients \(non encore concernés\)](#)

[Modèle TAC 13 pour aucun IOC / aucune version fixe disponible \(WAVE 2a — Await Fix\)](#)

[Modèle TAC 14 pour aucune version fixe/IOC disponible \(WAVE 2a — Mise à niveau immédiate\)](#)

[Modèle TAC 15 pour IOC Identified / Fixed Release disponible \(WAVE 2a — Urgent Upgrade\)](#)

[Modèle TAC 16 pour IOC identifié / Pas de version fixe disponible \(WAVE 2a — durcissement et correction d'attente\)](#)

Introduction

Ce document centralise les modèles d'e-mails approuvés par le client utilisés lors du triage et de la résolution des cas liés à la vulnérabilité de contournement d'authentification du contrôleur SD-WAN Cisco Catalyst. Les modèles sont divisés par expéditeur : Sherlock (échange automatique

de dossiers qui collecte les données admin-tech et renvoie les résultats préliminaires de l'IoC) et un ingénieur TAC (suivi humain pour l'investigation, la validation et la correction).

Références — Documentation Cisco SD-WAN CVE-2026-20182

Liste principale de tous les documents Cisco référencés dans les modèles d'e-mail ci-dessus. La numérotation est unifiée — par e-mail, les exposants (p. ex. ^[2]) pointent vers les éléments de cette liste.

1. **Guide de durcissement du SD-WAN de Cisco** — <https://sec.cloudapps.cisco.com/security/center/resources/Cisco-Catalyst-SD-WAN-HardeningGuide>
2. **Avis de sécurité officiel (cisco-sa-sdwan-mltnps2-JxpWm7R)** — <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-mltnps2-JxpWm7R>
3. **Guide de correction du TAC** — <https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/225842-remediate-catalyst-sd-wan-security.html#toc-h1d--1516256622>
4. **Guide de mise à niveau Cisco SD-WAN** — <https://www.cisco.com/c/en/us/support/docs/wan/dpt/220424-upgrade-sd-wan-controllers-with-the-use.html>
5. **Guide de collecte admin-tech pour Cisco SD-WAN** — <https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/216954-how-to-collect-an-admin-tech-in-an-sd-wa.html>
6. **Deuxième avis de sécurité (cisco-sa-sdwan-rpa2-v69WY2SW)** — <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa2-v69WY2SW>
7. **Lancez la mise à niveau de votre Catalyst SD-WAN** — <https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/225515-start-your-catalyst-sd-wan-upgrade.html>

E-mails

Sherlock 1 - Admission - Demande de mise à niveau et fichiers Admin-Tech

Scénario

Communication initiale lors de l'ouverture d'un dossier TAC pour le CVE-2026-20182 afin de conseiller la collecte de données admin-tech à partir de tous les composants de contrôle SD-WAN, puis leur mise à niveau.

Objet

Important : Action requise pour CVE-2026-20182 - Planification de la mise à niveau et évaluation de l'IoC

Message

Cher client,

Nous vous remercions d'avoir contacté le centre d'assistance technique Cisco (TAC).

En ce qui concerne la vulnérabilité associée au **CVE-2026-20182**, veuillez consulter l'[avis de sécurité officiel](#)^[1] pour obtenir des détails complets ainsi que le [guide de correction du TAC](#)^[2].

Notre objectif principal est de contribuer à sécuriser votre environnement. Veuillez **hiérarchiser la planification et l'exécution de votre mise à niveau** comme étant l'étape la plus importante pour limiter ce risque. Si vous n'avez pas encore planifié cette mise à niveau, veuillez le faire immédiatement.

Ressources de mise à niveau : Reportez-vous au document Cisco officiel suivant pour obtenir des instructions détaillées sur la façon d'effectuer la mise à niveau : [Guide de mise à niveau Cisco SD-WAN](#)^[3]

Pour permettre l'évaluation initiale de votre environnement pour tout indicateur de compromission potentiel (IoC) lié à CVE-2026-20182, vous devez effectuer une collecte admin-tech *avant* la mise à niveau. Veuillez suivre cet ordre d'opérations :

1. **Collecter les fichiers Admin-Tech** : Générez les journaux admin-tech à partir de tous les composants de contrôle SD-WAN avant la mise à niveau pour vous assurer qu'aucune donnée de diagnostic n'est perdue. Veillez à sélectionner à la fois "**Journaux**" et "**Technique**" lors de la génération de ces fichiers.
 - **vSmarts (contrôleurs)** : Collectez un à la fois, pas simultanément.
 - **vBonds (validateurs)** : Collecter à partir de tous les noeuds.
 - **Gestionnaire (vManage)** : Collecter à partir de tous les noeuds du cluster (DR actif et de secours).
2. **Exécuter la mise à niveau** : Mettez à niveau tous les composants de contrôle SD-WAN (vManage, vSmart, vBond) vers une version logicielle fixe répertoriée dans l'avis. N'attendez pas l'analyse du journal admin-tech avant de commencer la mise à niveau, car celle-ci ferme immédiatement la vulnérabilité.
3. **Télécharger vers le dossier TAC** : Une fois la mise à niveau terminée, téléchargez les fichiers précédemment collectés dans votre dossier TAC existant simultanément, si possible. Notre équipe analysera ensuite ces journaux afin d'évaluer votre environnement et de détecter d'éventuels indicateurs de compromission (IoC).

Ressources et assistance :

Pour plus d'informations et des instructions détaillées sur la génération et l'envoi sécurisé de vos fichiers admin-tech, reportez-vous à ce guide : [Guide de collecte admin-tech SD-WAN de Cisco](#)^[4].

Si vous êtes abonné au service BCS/LCS, contactez votre responsable de réseau ou de prestation Cisco pour obtenir des conseils supplémentaires sur le processus de mise à niveau ou les étapes suivantes.

La confidentialité et la sécurité de vos données restent notre priorité absolue. Toutes les informations fournies seront traitées conformément aux politiques de confidentialité et de sécurité de Cisco.

Vous recevrez un e-mail de confirmation automatique pour **CHAQUE** fichier téléchargé avec succès dans le dossier ; assurez-vous de vérifier ces notifications.

Merci de votre prompte coopération dans la sécurisation de votre infrastructure.

Liens :

[1] [Avis officiel sur la sécurité](#)

[2] [Guide de correction TAC](#)

[3] [Guide de mise à niveau Cisco SD-WAN](#)

[4] [Guide de collecte admin-tech SD-WAN de Cisco](#)

Cordialement,

Ouvrir dans Outlook

① Utilisez le téléchargement .eml ci-dessous. Remplacez tous les *[espaces réservés entre crochets]* avant l'envoi.

✉ Ouvrir Outlook (sujet uniquement)

⬇ Télécharger le modèle .eml

Sherlock 2 - Résultat - Aucune IoC observée (par fichier)

Scénario

Envoyé après l'analyse admin-tech, aucun indicateur de compromission n'est observé pour un fichier téléchargé spécifique. Envoyé une fois par fichier traité.

Objet

Mise à jour: Résultats d'analyse pour Composant SD-WAN [Insérer le nom du fichier] - CVE-2026-20182

Message

Cher client,

Merci de votre patience.

Nous avons terminé l'analyse du fichier admin-tech [Insérer le nom du fichier]. Dans ce fichier, nous n'avons pas identifié d'indicateurs de compromission liés à CVE-2026-20182 pour ce périphérique spécifique.

Veuillez noter que la quantité de données de journal que vous avez récupérées et fournies à Cisco pour cet examen peut avoir été limitée par la période de conservation des journaux que vous avez configurée conformément au **Guide de sécurisation SD-WAN de Cisco**^[1].

Important : Étapes suivantes et clôture du dossier :

1. **Attendre tous les résultats :** Veuillez noter que les résultats de cet e-mail peuvent être partiels. Nous analyserons chaque fichier tel qu'il est fourni. Veuillez attendre d'avoir reçu la confirmation de tous les fichiers téléchargés avant de considérer que l'évaluation est terminée.
2. **Priorité de mise à niveau :** Bien que les analyses préliminaires des journaux admin-tech n'aient pas identifié d'indicateurs de compromission (IoC), la vulnérabilité sous-jacente peut rester. Pour les déploiements Cisco Cloud-Pro et Cisco On-Prem, si vous ne l'avez pas encore fait, priorisez la mise à niveau complète de vos composants de contrôle SD-WAN dès que possible.
 - Cloud Cisco (fka : SaaS) sont automatiquement mis à niveau par Cisco dans le cadre du service géré. Aucune action requise.
3. **Clôture du dossier :** Une fois que vous avez reçu les résultats « aucune observation d'IoC » pour tous vos fichiers téléchargés ET (le cas échéant) que vous avez réussi la mise à niveau logicielle dans votre environnement, vous pouvez considérer ce cas résolu et poursuivre avec les procédures de fermeture standard.

Ressources de mise à niveau (le cas échéant) : Reportez-vous au document Cisco officiel suivant pour obtenir des instructions détaillées sur la mise à niveau de Cisco Cloud-Pro et de Cisco On-Prem : Guide de mise à niveau Cisco SD-WAN

Voici une présentation générale du processus de mise à niveau :

1. Téléchargement des images logicielles appropriées vers votre référentiel Manager (vManage).
2. Mise à niveau séquentielle de vos contrôleurs, en commençant par Manager (vManage), suivi de Validator (vBond) et Controller (vSmart).
3. Activation des nouvelles versions logicielles et validation du fonctionnement du système.

Nous continuerons à surveiller votre dossier. Si nous n'entendons pas de réponse dans les 10 jours ouvrables suivant la réception de tous les résultats basés sur les dossiers que nous avons reçus de votre part, nous supposons qu'aucune assistance supplémentaire n'est requise et nous procéderons aux procédures normales de clôture de cas du TAC. Si vous avez besoin d'aide, n'hésitez pas à nous le faire savoir.

Cordialement,

Ouvrir dans Outlook

① Remplacer tous les [espaces réservés entre crochets] avant l'envoi.

✉ Ouvrir Outlook (sujet uniquement)

↓ Télécharger le modèle .eml

Sherlock 3 - Rappel - Fichiers Admin-Tech manquants

Scénario

Suivi automatique lorsque les fichiers admin-tech soumis ne correspondent pas au nombre de composants de contrôle SD-WAN trouvés dans les journaux.

Objet

Rappel : Fichiers Admin-Tech manquants requis pour l'évaluation CVE-2026-20182

Message

Cher client,

Il nous manque encore des admin-techs dans vos composants de contrôle SD-WAN. Par conséquent, notre système ne peut pas évaluer les indicateurs de compromission dans les journaux admin-tech. Pour commencer l'évaluation CVE-2026-20182, nous devons recevoir des fichiers admin-tech de TOUS les contrôleurs (vSmarts), validateurs (vBonds) et gestionnaires (vManage), y compris tous les nœuds du gestionnaire (vManage) s'ils sont mis en cluster.

Étapes suivantes :

Veuillez télécharger les fichiers admin-tech restants le plus rapidement possible.

Cordialement,

Ouvrir dans Outlook

① Remplacer tous les [espaces réservés entre crochets] avant l'envoi.

✉ Ouvrir Outlook (avec le corps)

↓ Télécharger le modèle .eml

TAC 1 - Enquête - Examen supplémentaire requis (IoC suspecté)

Scénario

Envoyé par l'ingénieur du TAC une fois que l'automatisation a trouvé des journaux indiquant une éventuelle compromission et qu'une investigation humaine est requise.

Objet

N° SR - Enquête supplémentaire requise

Message

Cher client,

Mon nom est {your_name} et j'ai accepté votre demande. Nous vous remercions de votre collaboration continue avec le centre d'assistance technique de Cisco (TAC).

À la suite d'une analyse préliminaire des fichiers admin-tech que vous avez fournis à partir de **vos composants de contrôle SD-WAN**, nous avons identifié que d'autres investigations du TAC sont nécessaires pour compléter notre analyse. Afin de garantir une résolution complète et précise, je travaillerai en étroite collaboration avec vous sur les prochaines étapes.

Soyez assuré que nous nous engageons à vous soutenir tout au long de ces prochaines étapes et que nous vous fournirons des conseils clairs pour remédier à la situation de manière efficace.

Classez la planification et l'exécution de votre mise à niveau par ordre de priorité comme l'étape la plus importante pour limiter ce risque. Si vous n'avez pas encore planifié cette mise à niveau, veuillez le faire immédiatement.

Si vous avez des questions ou si vous avez besoin d'aide, n'hésitez pas à contacter votre ingénieur TAC.

Merci de votre attention et de votre collaboration.

Cordialement,

Ouvrir dans Outlook

① Remplacer tous les [espaces réservés entre crochets] avant l'envoi.

✉ Ouvrir Outlook (avec le corps)

↓ Télécharger le modèle .eml

TAC 2 - Résultat - Aucun IoC trouvé (confirmé par l'ingénieur)

Scénario

Envoyé par l'ingénieur TAC une fois que l'automatisation n'a détecté aucun indicateur de compromission et que l'ingénieur a confirmé le résultat.

Objet

Mise à jour: Examen du centre d'assistance technique terminé - Aucun IoC trouvé pour le CVE-2026-20182 - Dossier [SR #]

Message

Bonjour [Nom du client],

Je suis l'ingénieur du centre d'assistance technique Cisco affecté à votre dossier [numéro de demande de service].

Après avoir effectué une analyse préliminaire des fichiers admin-tech que vous avez fournis à partir de vos composants de contrôle SD-WAN, nous n'avons pas trouvé d'entrées de journal compatibles avec les indicateurs de compromission décrits dans les avis de sécurité SD-WAN de Cisco :

- **Vulnérabilité de contournement de l'authentification du contrôleur SD-WAN Cisco Catalyst [1]**
- **Vulnérabilités de Cisco Catalyst SD-WAN Manager [2]**

Cependant, vous devez procéder à la mise à niveau de tous vos composants de contrôle SD-WAN vers <insérer la version>. Voici les étapes à suivre pour procéder à la mise à niveau :

- **Lancez la mise à niveau de votre Catalyst SD-WAN [3]**
- **Guide de mise à niveau Cisco SD-WAN[4]**

Veuillez noter que Cisco n'est pas en mesure d'évaluer les journaux des périphériques de périphérie en raison de la nature dynamique de l'adressage IP sur Internet et de notre manque de connaissance des adresses IP attendues des périphériques de périphérie dans le réseau d'un client. Nous encourageons les clients à suivre les conseils de validation des événements d'appairage indiqués dans le document Cisco Catalyst SD-WAN Controller Authentication Bypass Vulnerability Security Advisory pour effectuer manuellement cette étape. Les clients sont également encouragés à effectuer les étapes de détection supplémentaires liées à la validation des événements d'appairage, comme décrit dans l'avis de sécurité pour CVE-2026-20182.

Liens

[1] Vulnérabilité de contournement de l'authentification du contrôleur SD-WAN Cisco Catalyst -

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa2-v69WY2SW>

[2] Vulnérabilités de Cisco Catalyst SD-WAN Manager -

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-mltnps2-JxpWm7R>

[3] Lancez la mise à niveau du SD-WAN Catalyst : <https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/225515->

<start-your-catalyst-sd-wan-upgrade.html>

[4] Guide de mise à niveau Cisco SD-WAN : <https://www.cisco.com/c/en/us/support/docs/wan/dpt/220424-upgrade-sd-wan-controllers-with-the-use.html>

Cordialement,

Ouvrir dans Outlook

① Remplacer tous les **[espaces réservés entre crochets]** avant l'envoi.

✉ Ouvrir Outlook (sujet uniquement)

↓ Télécharger le modèle .eml

TAC 3 - Validation - Confirmer la propriété IP dans la superposition

Scénario

Envoyé par un ingénieur TAC pour demander au client si des adresses IP spécifiques apparaissant lors de l'analyse du journal font ou faisaient partie de son infrastructure de superposition SD-WAN.

Objet

[N° SR] - Validation de l'adresse IP requise

Message

Cher/Chère [Nom du client],

Je m'appelle [Votre nom] et je suis l'ingénieur du centre d'assistance technique Cisco affecté à votre dossier.

Dans le cadre de notre analyse continue des fichiers admin-tech que vous avez fournis à partir de vos composants de contrôle SD-WAN, nous avons besoin de votre aide pour valider si les adresses IP suivantes font ou faisaient précédemment partie de votre infrastructure de superposition SD-WAN :

Adresse(s) IP en question :

- [Adresse IP 1]
- [Adresse IP 2]

Pour nous aider à terminer notre évaluation, veuillez confirmer :

1. Cette adresse IP est-elle actuellement associée à un composant de votre superposition SD-WAN (par exemple,

vManage, vSmart, vBond ou périphérique de périphérie) ?

2. Cette adresse IP a-t-elle déjà été utilisée par un composant de contrôle SD-WAN qui a été mis hors service ou dont l'adresse IP a été modifiée ?

3. Cette adresse IP est-elle associée à un site de reprise après sinistre (DR) ou à toute autre infrastructure liée à votre déploiement SD-WAN ?

Votre réponse rapide nous permettra de poursuivre notre analyse et de vous fournir les prochaines étapes appropriées.

Si vous avez des questions, n'hésitez pas à nous contacter.

Cordialement,

Ouvrir dans Outlook

① Remplacer tous les [espaces réservés entre crochets] avant l'envoi.

✉ Ouvrir Outlook (avec le corps)

⬇ Télécharger le modèle .eml

TAC 4 - Résultat - Faux positif effacé

Scénario

Envoyé par un ingénieur TAC après une vérification manuelle, il détermine que l'loC initial signalé par l'analyse automatisée était un faux positif.

Objet

Mise à jour: Examen technique pour CVE-2026-20182 - Dossier [Numéro de dossier]

Message

Cher client,

Nous vous remercions de votre patience pendant que notre équipe d'ingénierie effectuait une révision manuelle des fichiers admin-tech que vous avez fournis à partir de vos composants de contrôle SD-WAN.

À la suite d'une enquête approfondie, nous avons déterminé que l'indicateur initial de compromission (loC) signalé par notre processus d'analyse automatisée était un faux positif, c'est-à-dire que nous estimons que les loC ne sont pas valides.

Important : Bien que cette alerte spécifique ait été supprimée, veuillez noter que la vulnérabilité associée à [CVE-2026-](#)

[20182](#)^[1] nécessite une mise à niveau logicielle pour garantir la sécurité et l'intégrité à long terme de votre fabric SD-WAN.

Si vous n'avez pas encore terminé la mise à niveau : Veuillez donner la priorité à la mise à niveau complète de vos composants de contrôle SD-WAN dès que possible. La mise à niveau est le seul moyen de remédier efficacement à cette vulnérabilité. Reportez-vous au [Guide de mise à niveau Cisco SD-WAN](#)^[2] pour obtenir des instructions détaillées.

Si vous avez déjà effectué la mise à niveau : Puisque nous avons confirmé cette conclusion comme étant un faux positif et que vous avez déjà effectué la correction logicielle, aucune autre action n'est requise. Vous pouvez considérer ce cas résolu et poursuivre avec les procédures de fermeture standard.

Nous apprécions votre diligence à hiérarchiser la sécurité de votre infrastructure. Si vous avez d'autres questions ou si vous avez besoin d'aide supplémentaire, n'hésitez pas à nous contacter.

Cordialement,
Centre d'assistance technique Cisco (TAC)

Liens :

[1] [Avis officiel sur la sécurité](#)

[2] [Guide de mise à niveau Cisco SD-WAN](#)

Ouvrir dans Outlook

① Remplacer tous les **[espaces réservés entre crochets]** avant l'envoi.

✉ Ouvrir Outlook (sujet uniquement)

⬇ Télécharger le modèle .eml

TAC 5 - Critique - Identification de l'loC, appel de révision du calendrier

Scénario

Envoyé par un ingénieur du TAC lorsque des indicateurs de compromission potentiels ont été confirmés et qu'un appel urgent du client est requis pour discuter des conclusions et des étapes suivantes.

Objet

URGENT : Résultats de l'analyse pour CVE-2026-20182 - Indicateur de compromission identifié

Message

Cher client,

Merci de votre patience pendant que nous analysons les fichiers admin-tech fournis pour vos composants de contrôle SD-WAN.

À la suite de notre examen technique, nous avons identifié des indicateurs de compromission (IoC) potentiels liés au document CVE-2026-20182.

Compte tenu de la nature de ces résultats, il est essentiel que nous discutons des détails techniques et des prochaines étapes recommandées le plus tôt possible. Nous souhaiterions programmer un appel avec votre équipe pour passer en revue les résultats spécifiques et discuter des mesures correctives appropriées.

Étapes suivantes :

- **Réserver une téléconférence** : Veuillez nous faire part de votre disponibilité pour un bref appel dans les prochaines [p. ex., 4 à 8 heures] afin de passer en revue ces résultats.
- **Mise à niveau des composants de contrôle SDWAN** : Veuillez mettre à niveau votre gestionnaire, contrôleur et validateur SDWAN vers une version fixe dès que possible.

Notre objectif principal est de vous aider à sécuriser votre environnement et à limiter les risques potentiels. Nous apprécions votre prompt attention à cette question et nous nous réjouissons à l'idée de collaborer avec vous.

Cordialement,

Ouvrir dans Outlook

① Remplacer tous les *[espaces réservés entre crochets]* avant l'envoi.

✉ Ouvrir Outlook (avec le corps)

⬇ Télécharger le modèle .eml

TAC 6 - Résultat - IoC en double (Fermer et rediriger)

Scénario

Envoyé par un ingénieur TAC lorsque l'analyse de l'IoC confirme des résultats qui correspondent à une demande de service antérieure pour le même client/environnement. Le dossier en cours est clos et le client est redirigé vers la demande de service d'origine, où des conseils de correction ont déjà été fournis.

Objet

Mise à jour: Examen technique pour CVE-2026-20182 - Dossier [SR #] (confirmation de l'IoC en double)

Message

Cher client,

Merci de votre patience pendant que nous analysons les fichiers admin-tech fournis pour vos composants de contrôle SD-WAN. Nous avons déterminé que le ou les indicateurs de compromission (IoC) initiaux signalés par notre processus de numérisation sont les mêmes que ceux déjà communiqués dans **[Original SR #]**. Comme nous l'avons vu précédemment, nous vous recommandons de procéder à une mise à niveau urgente et de suivre l'une des deux procédures de correction décrites dans le [Guide de correction du TAC](#)^[2] afin de sécuriser votre environnement le plus rapidement possible. Reportez-vous à l'[avis de sécurité officiel pour CVE-2026-20182](#)^[1] pour plus de détails.

Je vais maintenant procéder à la clôture de ce dossier. Veuillez utiliser **[Original SR #]** pour demander des conseils ou une assistance technique supplémentaires concernant votre mise à niveau ou votre correction.

Cordialement,

[Votre nom]

Liens :

[1] [Avis officiel sur la sécurité](#)

[2] [Guide de correction TAC](#)

Ouvrir dans Outlook

① Remplacer tous les **[espaces réservés entre crochets]** avant l'envoi.

✉ Ouvrir Outlook (avec le corps)

⬇ Télécharger le modèle .eml

TAC 7 - Correction - Suivi des options (post-appel)

Scénario

Envoyé après l'appel d'examen de l'IoC pour récapituler les chemins de correction abordés. Le client choisit l'option A (redéploiement avec redémarrage progressif), l'option B (redéploiement avec basculement matériel) ou l'option C (reconstruction complète du système).

Objet

Suivi de la demande : Options de correction pour CVE-2026-20182

Message

Cher client,

Merci d'avoir pris le temps de discuter des résultats de notre récente analyse. Comme nous l'avons vu lors de l'appel

précédent, nous vous recommandons de suivre l'un des chemins de correction suivants pour sécuriser votre environnement.

Option A : Redéploiement avec redémarrage en continu. Priorise la continuité opérationnelle en évitant les temps d'arrêt du réseau, bien qu'elle comporte un risque résiduel de persistance des menaces pendant le processus de transition.

Description: Redéploiement du contrôleur, rotation des clés SSH et des certificats. Les composants de contrôleur existants sont connectés pendant la migration via vManage pour déployer le nouveau fabric, puis chacun est supprimé dès que le périphérique est migré.

Option B : Redéploiement avec basculement matériel. Fournit un niveau plus élevé d'assurance de sécurité. Comme les nouveaux contrôleurs ne se connectent jamais aux anciens, l'isolation est totale. Cela a un impact sur le fonctionnement global du réseau, car tous les périphériques doivent rétablir la connectivité et échanger des informations de routage/connectivité. Le temps d'indisponibilité dépend du nombre de sites, du nombre de préfixes échangés, etc.

Description: Redéploiement du contrôleur, rotation de la clé SSH et du certificat, mais les anciens composants du contrôleur sont isolés du nouveau fabric pendant le redéploiement.

Option C : Reconstruction complète du système. Fournit le plus haut niveau d'assurance de sécurité en établissant une base de référence propre, bien qu'il s'agisse de l'approche la plus complexe et qu'elle présente un risque plus élevé d'instabilité liée à la configuration pendant la reconstruction. Il s'agit d'une option de longue haleine qui nécessite une expertise dans la reconstruction des bases de données sur les modèles et les politiques.

Étapes suivantes :

- Veuillez discuter de ces options en interne et nous faire savoir quel chemin vous avez l'intention de prendre. Une fois que vous avez décidé, nous pouvons vous fournir des conseils supplémentaires ou une assistance technique pour vous aider tout au long de la phase d'exécution.

Nous sommes là pour vous accompagner tout au long de ce processus. N'hésitez pas à nous contacter si vous avez des questions concernant ces options.

Cordialement,
Centre d'assistance technique Cisco (TAC)

NOTE: L'option 1 était la mise à niveau. Le scénario considéré que cette mise à niveau a déjà été effectuée.

Ouvrir dans Outlook

① Utilisez le téléchargement .eml ci-dessous. Remplacez tous les *[espaces réservés entre crochets]* avant l'envoi.

✉ Ouvrir Outlook (sujet uniquement)

⬇ Télécharger le modèle .eml

TAC 8 - Correction - Options mises à jour pour les fabrics compromis (suivi de l'option 2)

Scénario

Informez les clients dont les structures SD-WAN ont été compromises et qui ont déjà fait l'objet de l'option 2 et dont les structures sont considérées comme présentant un risque de persistance des facteurs de menace. Les clients qui ont reconstruit leur fabric compromis (et qui ne s'appuyaient pas sur une sauvegarde/configDB existante) ne sont pas présumés être à risque et ne recevront pas cette communication. Cette communication sera envoyée par TBD.

Objet

Action urgente requise : Résolution des vulnérabilités critiques de l'infrastructure SD-WAN

Message

Cher client,

Nous fournissons une mise à jour critique pour la correction de votre fabric SD-WAN, comme indiqué dans [SR#] et les avis de sécurité communiqués précédemment. Cette mise à jour est spécifique aux tissus dans lesquels les journaux fournis ont montré des signes d'indicateurs de compromission (IOC).

Alors que vous aviez précédemment sélectionné un plan de correction basé sur l'option 2 (comportant une mise à niveau logicielle, un redéploiement du contrôleur et une rotation des clés SSH), notre analyse du paysage des menaces a continué à évoluer. De nouvelles connaissances techniques concernant l'exploitation de ces vulnérabilités indiquent que des mesures supplémentaires sont fortement recommandées pour réduire le risque de persistance et contribuer à assurer l'intégrité de la chaîne de confiance des certificats.

Mesure à prendre:

Nous avons mis à jour les stratégies de correction recommandées pour fournir une défense plus complète en incluant une rotation supplémentaire des certificats racine.

Veuillez noter que les corrections nécessiteront des activités de maintenance supplémentaires, pouvant inclure des interruptions planifiées du réseau.

Étant donné que notre priorité est la sécurité et l'intégrité de votre réseau, nous avons développé trois options de correction distinctes. Chaque option ci-dessous vous permet d'évaluer l'impact opérationnel par rapport à l'assurance de sécurité. Étant donné que votre position en matière de risque interne est unique, Cisco ne peut pas vous recommander un chemin particulier.

Option A : Redéploiement avec redémarrage en continu. Priorise la continuité opérationnelle en évitant les temps d'arrêt du réseau, bien qu'elle comporte un risque résiduel de persistance des menaces pendant le processus de transition.

Description: Redéploiement du contrôleur, rotation des clés SSH et des certificats. Les composants de contrôleur

existants sont connectés pendant la migration via vManage pour déployer le nouveau fabric, puis chacun est supprimé dès que le périphérique est migré.

Option B : Redéploiement avec basculement matériel. Fournit un niveau plus élevé d'assurance de sécurité.

Comme les nouveaux contrôleurs ne se connectent jamais aux anciens, l'isolation est totale. Cela a un impact sur le fonctionnement global du réseau, car tous les périphériques doivent rétablir la connectivité et échanger des informations de routage/connectivité. Le temps d'indisponibilité dépend du nombre de sites, du nombre de préfixes échangés, etc.

Description: Redéploiement du contrôleur, rotation de la clé SSH et du certificat, mais les anciens composants du contrôleur sont isolés du nouveau fabric pendant le redéploiement.

Option C : Reconstruction complète du système. Fournit le plus haut niveau d'assurance de sécurité en établissant une base de référence propre, bien qu'il s'agisse de l'approche la plus complexe et qu'elle présente un risque plus élevé d'instabilité liée à la configuration pendant la reconstruction. Il s'agit d'une option de longue haleine qui nécessite une expertise dans la reconstruction des bases de données sur les modèles et les politiques.

Une fois que votre équipe a examiné ces options et identifié l'approche qui correspond le mieux à vos normes de gestion des risques, veuillez nous le faire savoir en répondant à ce message. Après réception de votre sélection, nous coordonnerons la fenêtre de maintenance et commencerons les préparatifs techniques nécessaires à l'exécution.

Nous apprécions que vous continuiez à vous concentrer sur le maintien d'une infrastructure réseau sécurisée. Si vous avez besoin d'une clarification technique, veuillez nous en informer en envoyant une demande de service (SR) à notre Centre d'assistance technique (TAC).

Cordialement,
Cisco

Ouvrir dans Outlook

① Utilisez le téléchargement .eml ci-dessous. Remplacez tous les *[espaces réservés entre crochets]* avant l'envoi.

✉ Ouvrir Outlook (sujet uniquement)

⬇ Télécharger le modèle .eml

TAC 17 - Constatation inversée : auparavant, aucune IoC, maintenant identifiée (CVE-2026-20182)

Scénario

Envoyé aux clients **préalablement informés qu'aucun indicateur de compromission (IoC)** n'a été trouvé, mais pour lesquels un **examen interne ultérieur** des journaux admin-tech a depuis **identifié des indicateurs de compromission** liés à CVE-2026-20182. Communique la conclusion révisée et fournit les trois options de correction (option A, B ou C).

Objet

Mise à jour importante : Évaluation de l'IoC révisée pour CVE-2026-20182 - Les indicateurs de compromission sont maintenant identifiés - SR [SR#]

Message

Cher client,

Nous vous remercions de votre collaboration continue avec le centre d'assistance technique Cisco (TAC) concernant le CVE-2026-20182 dans le cadre de la demande de service [SR#].

Dans notre correspondance précédente, nous avons indiqué que notre analyse des fichiers admin-tech fournis par vos composants de contrôle SD-WAN n'avait pas identifié d'indicateurs de compromission (IoC) liés à cet avis. Dans le cadre de notre engagement continu envers votre sécurité, nous avons depuis effectué un examen interne de routine des données de journal admin-tech supplémentaires associées au fabric de votre organisation.

Cet examen ultérieur a permis d'identifier des indicateurs de compromission (IoC) qui n'ont pas été mis en évidence lors de l'évaluation initiale. Nous travaillons actuellement avec vous pour répondre à ces conclusions. Ces indicateurs de compromission indiquent une activité potentiellement suspecte au sein du fabric de votre entreprise qui nécessite des actions correctives.

Nous sommes conscients que cela modifie le résultat qui vous a été communiqué précédemment et nous voulons nous assurer que vous disposez d'une image claire et précise de votre environnement afin que les mesures correctives appropriées puissent être prises.

Mesure à prendre:

Veuillez noter que les corrections nécessiteront des activités de maintenance supplémentaires, pouvant inclure des interruptions planifiées du réseau.

Étant donné que notre priorité est la sécurité et l'intégrité de votre réseau, nous avons développé trois options de correction distinctes. Chaque option ci-dessous vous permet d'évaluer l'impact opérationnel par rapport à l'assurance de sécurité. Étant donné que votre position en matière de risque interne est unique, Cisco ne peut pas vous recommander un chemin particulier.

Option A : Redéploiement avec redémarrage en continu. Priorise la continuité opérationnelle en évitant les temps d'arrêt du réseau, bien qu'elle comporte un risque résiduel de persistance des menaces pendant le processus de transition.

Description: Redéploiement du contrôleur, rotation des clés SSH et des certificats. Les composants de contrôleur existants sont connectés pendant la migration via vManage pour déployer le nouveau fabric, puis chacun est supprimé dès que le périphérique est migré.

Option B : Redéploiement avec basculement matériel. Fournit un niveau plus élevé d'assurance de sécurité.

Comme les nouveaux contrôleurs ne se connectent jamais aux anciens, l'isolation est totale. Cela a un impact sur le fonctionnement global du réseau, car tous les périphériques doivent rétablir la connectivité et échanger des informations de routage/connectivité. Le temps d'indisponibilité dépend du nombre de sites, du nombre de préfixes échangés, etc.

Description: Redéploiement du contrôleur, rotation de la clé SSH et du certificat, mais les anciens composants du contrôleur sont isolés du nouveau fabric pendant le redéploiement.

Option C : Reconstruction complète du système. Fournit le plus haut niveau d'assurance de sécurité en établissant une base de référence propre, bien qu'il s'agisse de l'approche la plus complexe et qu'elle présente un risque plus élevé d'instabilité liée à la configuration pendant la reconstruction. Il s'agit d'une option de longue haleine qui nécessite une expertise dans la reconstruction des bases de données des modèles et des politiques.

Une fois que votre équipe a examiné ces options et identifié l'approche qui correspond le mieux à vos normes de gestion des risques, veuillez nous le faire savoir en répondant à ce message. Après réception de votre sélection, nous coordonnerons la fenêtre de maintenance et commencerons les préparatifs techniques nécessaires à l'exécution.

Nous apprécions que vous continuiez à vous concentrer sur le maintien d'une infrastructure réseau sécurisée. Veuillez nous faire savoir si vous avez besoin de plus de précisions techniques en répondant à cet e-mail ou par le biais de la demande de service (SR) existante auprès de notre Centre d'assistance technique (TAC).

Cordialement,
Cisco

Ouvrir dans Outlook

① Utilisez le téléchargement .eml ci-dessous. Remplacez tous les *[espaces réservés entre crochets]* avant l'envoi.

✉ Ouvrir Outlook (sujet uniquement)

⬇ Télécharger le modèle .eml

CloudOps 1 - Proactive - IoC détecté dans l'analyse du cloud, Admin-Tech requis pour la validation

Scénario

Envoyé de manière proactive lorsqu'une analyse de sécurité Cisco CloudOps d'un fabric SD-WAN hébergé dans le cloud a fait apparaître des indicateurs de compromission potentiels. Une demande de service est ouverte pour le compte du client et ce dernier est invité à joindre des fichiers admin-tech afin que la conclusion puisse être validée par une analyse complète du journal.

Objet

Mesure à prendre: Fichiers Admin-Tech nécessaires à la validation des résultats de l'analyse de sécurité - SR [SR#]

Message

Cher client,

Dans le cadre de notre engagement continu à sécuriser et à surveiller l'intégrité des offres Cisco, Cisco a récemment effectué une analyse de sécurité de certains fabric SD-WAN hébergés dans le cloud. Cette mesure a été prise en réponse à un problème de sécurité signalé. L'analyse a identifié une activité potentiellement suspecte dans le fabric de votre organisation qui mérite un examen plus approfondi.

Nous vous demandons de nous aider à joindre des fichiers admin-tech à cette demande de service (SR), qui a été ouverte en votre nom, afin que nous puissions valider cette conclusion et terminer notre enquête.

Pour permettre une analyse complète, collectez et téléchargez des fichiers admin-tech à partir de tous les composants de contrôle SD-WAN. Veuillez à sélectionner à la fois "**Journaux**" et "**Tech**" lors de la génération de ces fichiers :

- **vSmarts (contrôleurs)** : Collectez un à la fois, pas simultanément.
- **vBonds (validateurs)** : Collecter à partir de tous les noeuds.
- **Gestionnaire (vManage)** : Collecter à partir de tous les noeuds du cluster (DR actif et de secours).

Pour obtenir des instructions détaillées étape par étape sur la génération et l'envoi sécurisé de vos fichiers admin-tech, reportez-vous à ce guide : [Guide de collecte admin-tech SD-WAN de Cisco](#)^[1].

Une fois que nous recevons les fichiers demandés, notre équipe les analysera pour confirmer si l'activité observée représente un véritable indicateur de compromission et vous conseillera sur les prochaines étapes appropriées.

Nous apprécions que vous continuiez à vous concentrer sur le maintien d'une infrastructure réseau sécurisée. Veuillez nous faire savoir si vous avez besoin de plus de précisions techniques en répondant à cette demande de service.

Cordialement,
Cisco

Liens :

[1] [Guide de collecte admin-tech SD-WAN de Cisco](#)

Ouvrir dans Outlook

① Utilisez le téléchargement .eml ci-dessous. Remplacez tous les **[espaces réservés entre crochets]** avant l'envoi.

✉ Ouvrir Outlook (sujet uniquement)

⬇ Télécharger le modèle .eml

E-mails pour la VAGUE 2A pour les clients PRÉCÉDEMMENT CONCERNÉS qui n'ont pas déjà complété les options A, B ou C.

(Les options 1 et 2 doivent être refaites)

Modèle TAC 9 pour aucun CIO pour PSIRT2a/ils ont reconstruit
(**PRÉCÉDEMMENT IMPACTÉ**)

Scénario

Envoyé aux clients dont les journaux SD-WAN **ne** présentaient **aucun indicateur de compromission (IoC)** lié à l'avis PSIRT2a ET qui ont **précédemment reconstruit** leur fabric. Fournit des conseils de correction mis à jour avec trois options (suivi de l'option 2).

Objet

Action urgente requise : Résolution des vulnérabilités critiques de l'infrastructure SD-WAN - SR [SR#]

Message

Cher client,

Nous vous remercions d'avoir contacté le centre d'assistance technique Cisco (TAC) au sujet des récents avis PSIRT SD-WAN dans le cadre de la demande de service [SR#].

Après avoir examiné les journaux et les informations fournis par votre fabric SD-WAN, notre analyse n'a identifié aucun indicateur de compromission (IOC) associé à l'avis de vulnérabilité SD-WAN du 5 juin 2026. De plus, nous savons que votre environnement a déjà été reconstruit dans le cadre d'efforts de correction liés à des avis antérieurs.

Nous aimerions vous faire part d'une mise à jour importante concernant les recommandations de correction pour les fabrics SD-WAN en tenant compte des nouvelles informations identifiées en rapport avec ces vulnérabilités.

Nous fournissons une mise à jour critique pour la correction de votre fabric SD-WAN, comme indiqué dans [SR#] et les avis de sécurité communiqués précédemment.

Alors que vous aviez précédemment sélectionné un plan de correction basé sur l'option 2 (comprenant une mise à niveau logicielle, un redéploiement du contrôleur et une rotation des clés SSH), notre analyse du paysage des menaces a continué à évoluer. De nouvelles connaissances techniques concernant l'exploitation de ces vulnérabilités indiquent que des mesures supplémentaires sont fortement recommandées pour réduire le risque de persistance et contribuer à assurer l'intégrité de la chaîne de confiance des certificats.

Mesure à prendre:

Nous avons mis à jour les stratégies de correction recommandées pour fournir une défense plus complète en incluant une rotation supplémentaire des certificats racine.

Veuillez noter que les corrections nécessiteront des activités de maintenance supplémentaires, pouvant inclure des

interruptions planifiées du réseau. Étant donné que notre priorité est la sécurité et l'intégrité de votre réseau, nous avons développé trois options de correction distinctes. Chaque option ci-dessous vous permet d'évaluer l'impact opérationnel par rapport à l'assurance de sécurité. Étant donné que votre position en matière de risque interne est unique, Cisco ne peut pas vous recommander un chemin particulier.

Option A : Redéploiement avec redémarrage en continu. Priorise la continuité opérationnelle en évitant les temps d'arrêt du réseau, bien qu'elle comporte un risque résiduel de persistance des menaces pendant le processus de transition.

Description: Redéploiement du contrôleur, rotation des clés SSH et des certificats. Les composants de contrôleur existants sont connectés pendant la migration via vManage pour déployer le nouveau fabric, puis chacun est supprimé dès que le périphérique est migré.

Option B : Redéploiement avec basculement matériel. Fournit un niveau plus élevé d'assurance de sécurité. Comme les nouveaux contrôleurs ne se connectent jamais aux anciens, l'isolation est totale. Cela a un impact sur le fonctionnement global du réseau, car tous les périphériques doivent rétablir la connectivité et échanger des informations de routage/connectivité. Le temps d'indisponibilité dépend du nombre de sites, du nombre de préfixes échangés, etc.

Description: Redéploiement du contrôleur, rotation de la clé SSH et du certificat, mais les anciens composants du contrôleur sont isolés du nouveau fabric pendant le redéploiement.

Option C : Reconstruction complète du système. Fournit le plus haut niveau d'assurance de sécurité en établissant une base de référence propre, bien qu'il s'agisse de l'approche la plus complexe et qu'elle présente un risque plus élevé d'instabilité liée à la configuration pendant la reconstruction. Il s'agit d'une option de longue haleine qui nécessite une expertise dans la reconstruction des bases de données des modèles et des politiques.

Une fois que votre équipe a examiné ces options et identifié l'approche qui correspond le mieux à vos normes de gestion des risques, veuillez nous le faire savoir en répondant à ce message. Après réception de votre sélection, nous coordonnerons la fenêtre de maintenance et commencerons les préparatifs techniques nécessaires à l'exécution.

Nous apprécions que vous continuiez à vous concentrer sur le maintien d'une infrastructure réseau sécurisée. Veuillez nous faire savoir si vous avez besoin de plus de précisions techniques en répondant à cet e-mail ou via la demande de service existante.

Cordialement,
Cisco

Ouvrir dans Outlook

① Utilisez le téléchargement .eml ci-dessous. Remplacez tous les *[espaces réservés entre crochets]* avant l'envoi.

✉ Ouvrir Outlook (sujet uniquement)

⬇ Télécharger le modèle .eml

Modèle TAC 10 pour oui COI pour PSIRT2a/ils ont reconstruit (**PRÉCÉDEMMENT IMPACTÉ**)

Scénario

Envoyé aux clients dont les journaux SD-WAN affichaient **des indicateurs de compromission (IoC)** liés à l'avis PSIRT2a ET qui ont **précédemment reconstruit** leur fabric. Fournit des conseils de correction mis à jour avec trois options (suivi de l'option 2).

Objet

Action urgente requise : Résolution des vulnérabilités critiques de l'infrastructure SD-WAN - SR [SR#]

Message

Cher client,

Nous vous remercions d'avoir contacté le centre d'assistance technique Cisco (TAC) au sujet des récents avis PSIRT SD-WAN dans le cadre de la demande de service [SR#].

Après avoir analysé les journaux fournis par votre fabric SD-WAN, notre équipe a identifié des indicateurs de compromission (IOC) associés à l'avis de vulnérabilité SD-WAN du 5 juin 2026. Nous comprenons également que votre environnement a déjà été reconstruit dans le cadre des étapes de correction liées aux avis précédents.

Nous fournissons une mise à jour critique pour la correction de votre fabric SD-WAN, comme indiqué dans [SR#] et les avis de sécurité communiqués précédemment. Cette mise à jour est spécifique aux tissus dans lesquels les journaux fournis ont montré des signes d'indicateurs de compromission (IOC).

Alors que vous aviez précédemment sélectionné un plan de correction basé sur l'option 2 (comprenant une mise à niveau logicielle, un redéploiement du contrôleur et une rotation des clés SSH), notre analyse du paysage des menaces a continué à évoluer. De nouvelles connaissances techniques concernant l'exploitation de ces vulnérabilités indiquent que des mesures supplémentaires sont fortement recommandées pour réduire le risque de persistance et contribuer à assurer l'intégrité de la chaîne de confiance des certificats.

Mesure à prendre:

Nous avons mis à jour les stratégies de correction recommandées pour fournir une défense plus complète en incluant une rotation supplémentaire des certificats racine.

Veuillez noter que les corrections nécessiteront des activités de maintenance supplémentaires, pouvant inclure des interruptions planifiées du réseau. Étant donné que notre priorité est la sécurité et l'intégrité de votre réseau, nous avons développé trois options de correction distinctes. Chaque option ci-dessous vous permet d'évaluer l'impact opérationnel par rapport à l'assurance de sécurité. Étant donné que votre position en matière de risque interne est unique, Cisco ne peut pas vous recommander un chemin particulier.

Option A : Redéploiement avec redémarrage en continu. Priorise la continuité opérationnelle en évitant les temps

d'arrêt du réseau, bien qu'elle comporte un risque résiduel de persistance des menaces pendant le processus de transition.

Description: Redéploiement du contrôleur, rotation des clés SSH et des certificats. Les composants de contrôleur existants sont connectés pendant la migration via vManage pour déployer le nouveau fabric, puis chacun est supprimé dès que le périphérique est migré.

Option B : Redéploiement avec basculement matériel. Fournit un niveau plus élevé d'assurance de sécurité.

Comme les nouveaux contrôleurs ne se connectent jamais aux anciens, l'isolation est totale. Cela a un impact sur le fonctionnement global du réseau, car tous les périphériques doivent rétablir la connectivité et échanger des informations de routage/connectivité. Le temps d'indisponibilité dépend du nombre de sites, du nombre de préfixes échangés, etc.

Description: Redéploiement du contrôleur, rotation de la clé SSH et du certificat, mais les anciens composants du contrôleur sont isolés du nouveau fabric pendant le redéploiement.

Option C : Reconstruction complète du système. Fournit le plus haut niveau d'assurance de sécurité en établissant une base de référence propre, bien qu'il s'agisse de l'approche la plus complexe et qu'elle présente un risque plus élevé d'instabilité liée à la configuration pendant la reconstruction. Il s'agit d'une option de longue haleine qui nécessite une expertise dans la reconstruction des bases de données des modèles et des politiques.

Une fois que votre équipe a examiné ces options et identifié l'approche qui correspond le mieux à vos normes de gestion des risques, veuillez nous le faire savoir en répondant à ce message. Après réception de votre sélection, nous coordonnerons la fenêtre de maintenance et commencerons les préparatifs techniques nécessaires à l'exécution.

Nous apprécions que vous continuiez à vous concentrer sur le maintien d'une infrastructure réseau sécurisée. Veuillez nous faire savoir si vous avez besoin de plus de précisions techniques en répondant à cet e-mail ou via la demande de service existante.

Cordialement,
Cisco

Ouvrir dans Outlook

① Utilisez le téléchargement .eml ci-dessous. Remplacez tous les [espaces réservés entre crochets] avant l'envoi.

✉ Ouvrir Outlook (sujet uniquement)

⬇ Télécharger le modèle .eml

Modèle TAC 11 pour aucun CIO pour PSIRT2a/ils n'ont pas reconstruit
(PRÉCÉDEMMENT IMPACTÉ)

Scénario

Envoyé aux clients dont les journaux SD-WAN **ne** présentaient **aucun indicateur de compromission (IoC)** lié à l'avis PSIRT2a ET qui **n'ont PAS reconstruit** leur fabric. Fournit des conseils de correction mis à jour avec trois options (suivi de l'option 1).

Objet

Action urgente requise : Résolution des vulnérabilités critiques de l'infrastructure SD-WAN - SR [SR#]

Message

Cher client,

Nous vous remercions d'avoir contacté le centre d'assistance technique Cisco (TAC) au sujet des récents avis PSIRT SD-WAN dans le cadre de la demande de service [SR#].

Après avoir examiné les journaux et les informations fournis par votre fabric SD-WAN, nous n'avons pas identifié d'indicateurs de compromission (IOC) associés à l'avis de vulnérabilité SD-WAN du 5 juin 2026.

Nous comprenons également que votre environnement n'a pas subi une reconstruction complète suite aux avis précédents. Cisco recommande d'examiner les conseils de correction mis à jour ci-dessous afin de réduire l'exposition potentielle et de renforcer l'intégrité de la chaîne de confiance du certificat SD-WAN.

Dans cet esprit, nous vous fournissons une mise à jour critique pour la correction de votre fabric SD-WAN, comme indiqué dans [SR#] et les avis de sécurité précédemment communiqués.

Alors que vous aviez précédemment sélectionné un plan de correction basé sur l'option 1 (comportant une mise à niveau logicielle et une rotation des clés SSH), notre analyse du paysage des menaces a continué à évoluer. De nouvelles connaissances techniques concernant l'exploitation de ces vulnérabilités indiquent que des mesures supplémentaires sont fortement recommandées pour réduire le risque de persistance et contribuer à assurer l'intégrité de la chaîne de confiance des certificats.

Mesure à prendre:

Nous avons mis à jour les stratégies de correction recommandées pour fournir une défense plus complète en incluant une rotation supplémentaire des certificats racine.

Veuillez noter que les corrections nécessiteront des activités de maintenance supplémentaires, pouvant inclure des interruptions planifiées du réseau. Étant donné que notre priorité est la sécurité et l'intégrité de votre réseau, nous avons développé trois options de correction distinctes. Chaque option ci-dessous vous permet d'évaluer l'impact opérationnel par rapport à l'assurance de sécurité. Étant donné que votre position en matière de risque interne est unique, Cisco ne peut pas vous recommander un chemin particulier.

Option A : Redéploiement avec redémarrage en continu. Priorise la continuité opérationnelle en évitant les temps d'arrêt du réseau, bien qu'elle comporte un risque résiduel de persistance des menaces pendant le processus de transition.

Description: Redéploiement du contrôleur, rotation des clés SSH et des certificats. Les composants de contrôleur existants sont connectés pendant la migration via vManage pour déployer le nouveau fabric, puis chacun est supprimé dès que le périphérique est migré.

Option B : Redéploiement avec basculement matériel. Fournit un niveau plus élevé d'assurance de sécurité. Comme les nouveaux contrôleurs ne se connectent jamais aux anciens, l'isolation est totale. Cela a un impact sur le fonctionnement global du réseau, car tous les périphériques doivent rétablir la connectivité et échanger des informations de routage/connectivité. Le temps d'indisponibilité dépend du nombre de sites, du nombre de préfixes échangés, etc.

Description: Redéploiement du contrôleur, rotation de la clé SSH et du certificat, mais les anciens composants du contrôleur sont isolés du nouveau fabric pendant le redéploiement.

Option C : Reconstruction complète du système. Fournit le plus haut niveau d'assurance de sécurité en établissant une base de référence propre, bien qu'il s'agisse de l'approche la plus complexe et qu'elle présente un risque plus élevé d'instabilité liée à la configuration pendant la reconstruction. Il s'agit d'une option de longue haleine qui nécessite une expertise dans la reconstruction des bases de données des modèles et des politiques.

Une fois que votre équipe a examiné ces options et identifié l'approche qui correspond le mieux à vos normes de gestion des risques, veuillez nous le faire savoir en répondant à ce message. Après réception de votre sélection, nous coordonnerons la fenêtre de maintenance et commencerons les préparatifs techniques nécessaires à l'exécution.

Nous apprécions que vous continuiez à vous concentrer sur le maintien d'une infrastructure réseau sécurisée. Veuillez nous faire savoir si vous avez besoin de plus de précisions techniques en répondant à cet e-mail ou via la demande de service existante.

Cordialement,
Cisco

Ouvrir dans Outlook

① Utilisez le téléchargement .eml ci-dessous. Remplacez tous les *[espaces réservés entre crochets]* avant l'envoi.

✉ Ouvrir Outlook (sujet uniquement)

⬇ Télécharger le modèle .eml

Modèle TAC 12 pour oui COI pour PSIRT2a/ils n'ont pas reconstruit (PRÉCÉDEMMENT IMPACTÉ)

Scénario

Envoyé aux clients dont les journaux SD-WAN indiquaient **des indicateurs de compromission (IoC)** liés à l'avis PSIRT2a ET qui **n'ont PAS reconstruit** leur fabric. Fournit des conseils de correction mis à jour avec trois options (suivi de l'option 1).

Objet

Action urgente requise : Résolution des vulnérabilités critiques de l'infrastructure SD-WAN - SR [SR#]

Message

Cher client,

Nous vous remercions d'avoir contacté le centre d'assistance technique Cisco (TAC) au sujet des récents avis PSIRT SD-WAN dans le cadre de la demande de service [SR#].

Après avoir analysé les journaux fournis par votre fabric SD-WAN, notre équipe a identifié des indicateurs de compromission (IOC) associés à l'avis de vulnérabilité SD-WAN du 5 juin 2026. De plus, nous savons que votre environnement n'a pas été entièrement reconstruit suite aux avis précédents.

Étant donné la présence de ces indicateurs et l'évolution de la compréhension du paysage des menaces, il est important d'examiner et de mettre en oeuvre les conseils de correction mis à jour décrits ci-dessous afin de réduire le risque de persistance et de garantir l'intégrité de votre chaîne de confiance de certificat SD-WAN.

Nous fournissons une mise à jour critique pour la correction de votre fabric SD-WAN, comme indiqué dans [SR#] et les avis de sécurité communiqués précédemment. Cette mise à jour est spécifique aux tissus dans lesquels les journaux fournis ont montré des signes d'indicateurs de compromission (IOC).

Alors que vous aviez précédemment sélectionné un plan de correction basé sur l'option 1 (comportant une mise à niveau logicielle et une rotation des clés SSH), notre analyse du paysage des menaces a continué à évoluer. De nouvelles connaissances techniques concernant l'exploitation de ces vulnérabilités indiquent que des mesures supplémentaires sont fortement recommandées pour réduire le risque de persistance et contribuer à assurer l'intégrité de la chaîne de confiance des certificats.

Mesure à prendre:

Nous avons mis à jour les stratégies de correction recommandées pour fournir une défense plus complète en incluant une rotation supplémentaire des certificats racine.

Veuillez noter que les corrections nécessiteront des activités de maintenance supplémentaires, pouvant inclure des interruptions planifiées du réseau. Étant donné que notre priorité est la sécurité et l'intégrité de votre réseau, nous avons développé trois options de correction distinctes. Chaque option ci-dessous vous permet d'évaluer l'impact opérationnel par rapport à l'assurance de sécurité. Étant donné que votre position en matière de risque interne est unique, Cisco ne peut pas vous recommander un chemin particulier.

Option A : Redéploiement avec redémarrage en continu. Priorise la continuité opérationnelle en évitant les temps d'arrêt du réseau, bien qu'elle comporte un risque résiduel de persistance des menaces pendant le processus de transition.

Description: Redéploiement du contrôleur, rotation des clés SSH et des certificats. Les composants de contrôleur

existants sont connectés pendant la migration via vManage pour déployer le nouveau fabric, puis chacun est supprimé dès que le périphérique est migré.

Option B : Redéploiement avec basculement matériel. Fournit un niveau plus élevé d'assurance de sécurité.

Comme les nouveaux contrôleurs ne se connectent jamais aux anciens, l'isolation est totale. Cela a un impact sur le fonctionnement global du réseau, car tous les périphériques doivent rétablir la connectivité et échanger des informations de routage/connectivité. Le temps d'indisponibilité dépend du nombre de sites, du nombre de préfixes échangés, etc.

Description: Redéploiement du contrôleur, rotation de la clé SSH et du certificat, mais les anciens composants du contrôleur sont isolés du nouveau fabric pendant le redéploiement.

Option C : Reconstruction complète du système. Fournit le plus haut niveau d'assurance de sécurité en établissant une base de référence propre, bien qu'il s'agisse de l'approche la plus complexe et qu'elle présente un risque plus élevé d'instabilité liée à la configuration pendant la reconstruction. Il s'agit d'une option de longue haleine qui nécessite une expertise dans la reconstruction des bases de données des modèles et des politiques.

Une fois que votre équipe a examiné ces options et identifié l'approche qui correspond le mieux à vos normes de gestion des risques, veuillez nous le faire savoir en répondant à ce message. Après réception de votre sélection, nous coordonnerons la fenêtre de maintenance et commencerons les préparatifs techniques nécessaires à l'exécution.

Nous apprécions que vous continuiez à vous concentrer sur le maintien d'une infrastructure réseau sécurisée. Veuillez nous faire savoir si vous avez besoin de plus de précisions techniques en répondant à cet e-mail ou via la demande de service existante.

Cordialement,
Cisco

Ouvrir dans Outlook

① Utilisez le téléchargement .eml ci-dessous. Remplacez tous les *[espaces réservés entre crochets]* avant l'envoi.

✉ Ouvrir Outlook (sujet uniquement)

⬇ Télécharger le modèle .eml

E-mails pour la VAGUE 2A pour les NOUVEAUX clients (non encore concernés)

Modèle TAC 13 pour aucun IOC / aucune version fixe disponible (WAVE 2a — Await Fix)

Scénario

Envoyé aux clients dont les journaux SD-WAN ne présentaient **aucun indicateur de compromission (IoC)** lié au CVE-2026-20245, mais pour lesquels **aucune version logicielle fixe n'est actuellement disponible** pour leur plate-forme/version. Conseille au client d'appliquer des mesures de durcissement provisoires et d'attendre la notification de libération fixe.

Objet

Mise à jour: Évaluation de l'IoC terminée pour CVE-2026-20245 - Aucune version fixe actuellement disponible - SR [SR#]

Message

Cher client,

Nous vous remercions d'avoir contacté le centre d'assistance technique Cisco (TAC) pour le document CVE-2026-20245 dans la section Demande de service [SR#].

Nous avons terminé l'analyse des fichiers admin-tech que vous avez fournis à partir de vos composants de contrôle SD-WAN. **Nous n'avons identifié aucun indicateur de compromission (IoC)** associé à CVE-2026-20245 dans les journaux examinés.

Veuillez noter que la quantité de données de journal récupérées et fournies à Cisco pour cet examen peut avoir été limitée par la période de conservation des journaux configurée dans votre environnement conformément au [Guide de sécurisation SD-WAN de Cisco](#)^[1].

Important — Aucune Version De Logiciel Fixe Actuellement Disponible :

Pour le moment, **aucune version logicielle fixe n'est disponible** pour votre plate-forme et votre version logicielle actuelles afin de remédier à cette vulnérabilité. L'équipe d'ingénierie de Cisco travaille activement à fournir une version fixe. Une fois que le logiciel fixe sera disponible, l'[avis de sécurité officiel](#)^[2] sera mis à jour avec les informations de version fixe.

Mesures provisoires recommandées :

En attendant la version fixe, nous vous recommandons fortement de mettre en oeuvre les mesures de durcissement suivantes pour réduire votre exposition :

- 1. Appliquer les meilleures pratiques de renforcement :** Examinez et mettez en oeuvre les recommandations du [Guide de durcissement du SD-WAN de Cisco](#)^[1] pour réduire votre surface d'attaque.
- 2. Surveiller les conseils de sécurité :** Consultez régulièrement l'[avis de sécurité officiel](#)^[2] pour obtenir des mises à jour sur la disponibilité des versions fixes de votre plate-forme.
- 3. Planification de la mise à niveau :** Commencez dès maintenant la planification de la mise à niveau afin d'être prêt à exécuter la mise à niveau rapidement une fois la version corrigée publiée.
- 4. Surveillez votre environnement :** Continuez à surveiller vos composants de contrôle SD-WAN pour détecter tout comportement anormal ou toute modification de configuration inattendue.

Étapes suivantes :

Nous mettrons à jour ce dossier lorsque la version logicielle fixe sera disponible. À ce stade, vous devez donner la priorité à la mise à niveau de tous les composants de contrôle SD-WAN (gestionnaire, contrôleur, validateur) vers la version fixe dès que possible.

Si vous êtes abonné au programme BCS/LCS, contactez votre responsable de réseau ou de prestation Cisco pour obtenir des conseils supplémentaires sur la planification de la mise à niveau.

Nous apprécions votre patience et votre engagement envers la sécurité de votre infrastructure. Si vous avez des questions ou si vous avez besoin d'aide supplémentaire dans l'intervalle, n'hésitez pas à répondre à ce cas.

Cordialement,
Centre d'assistance technique Cisco (TAC)

Liens :

[1] [Guide de sécurisation du SD-WAN de Cisco](#)

[2] [Avis de sécurité officiel \(cisco-sa-sdwan-privesc-4uxFrdzx\)](#)

Ouvrir dans Outlook

① Remplacer tous les **[espaces réservés entre crochets]** avant l'envoi.

✉ Ouvrir Outlook (sujet uniquement)

⬇ Télécharger le modèle .eml

Modèle TAC 14 pour aucune version fixe/IOC disponible (WAVE 2a — Mise à niveau immédiate)

Scénario

Envoyé aux clients dont les journaux SD-WAN **ne** contenaient **aucun indicateur de compromission (IoC)** lié au CVE-2026-20245 ET pour lesquels une **version logicielle fixe est disponible**. Conseille au client de procéder immédiatement à la planification et à l'exécution de la mise à niveau.

Objet

Mise à jour: Évaluation de l'IoC terminée pour CVE-2026-20245 - Aucun IoC trouvé, mise à niveau requise - SR [SR#]

Message

Cher client,

Nous vous remercions d'avoir contacté le centre d'assistance technique Cisco (TAC) pour le document CVE-2026-20245 dans la section Demande de service [SR#].

Nous avons terminé l'analyse des fichiers admin-tech que vous avez fournis à partir de vos composants de contrôle SD-WAN. **Nous n'avons identifié aucun indicateur de compromission (IoC)** associé à CVE-2026-20245 dans les journaux examinés.

Veillez noter que la quantité de données de journal récupérées et fournies à Cisco pour cet examen peut avoir été limitée par la période de conservation des journaux configurée dans votre environnement conformément au [Guide de sécurisation SD-WAN de Cisco](#)^[1].

Important — Mise à niveau requise :

Bien qu'aucun IoC n'ait été identifié, la vulnérabilité sous-jacente reste présente jusqu'à ce que vos composants de contrôle SD-WAN soient mis à niveau vers une version logicielle fixe. Une version fixe est désormais disponible pour votre plate-forme.

Veillez **classer votre planification et votre exécution de mise à niveau** par ordre de priorité comme l'étape la plus importante pour remédier à cette vulnérabilité. Si vous n'avez pas encore planifié cette mise à niveau, veuillez le faire immédiatement.

Étapes suivantes :

1. **Mise à niveau de tous les composants de contrôle SD-WAN :** Mettez à niveau votre Manager (vManage), votre Controller (vSmart) et votre Validator (vBond) vers une version logicielle fixe répertoriée dans l'[avis de sécurité officiel](#)^[2].
2. **Ressources de mise à niveau :** Reportez-vous aux documents Cisco officiels suivants pour obtenir des instructions détaillées sur la mise à niveau :
 - [Lancez la mise à niveau de votre Catalyst SD-WAN](#)^[3]
 - [Guide de mise à niveau Cisco SD-WAN](#)^[4]
3. **Clôture du dossier :** Une fois la mise à niveau du logiciel terminée dans votre environnement, vous pouvez envisager de résoudre ce problème et de poursuivre les procédures de fermeture standard.

Si vous êtes abonné à BCS/LCS, contactez votre responsable de réseau ou de prestation Cisco pour obtenir des conseils supplémentaires sur le processus de mise à niveau.

Nous continuerons à surveiller votre dossier. Si nous n'avons pas de réponse dans les 10 jours ouvrables, nous supposerons qu'aucune assistance supplémentaire n'est requise et nous procéderons aux procédures normales de clôture des dossiers du TAC.

Cordialement,

Centre d'assistance technique Cisco (TAC)

Liens :

- [1] [Guide de sécurisation du SD-WAN de Cisco](#)
- [2] [Avis de sécurité officiel \(cisco-sa-sdwan-privesc-4uxFrdzx\)](#)
- [3] [Commencez votre mise à niveau Catalyst SD-WAN](#)
- [4] [Guide de mise à niveau Cisco SD-WAN](#)

Ouvrir dans Outlook

① Remplacer tous les [espaces réservés entre crochets] avant l'envoi.

✉ Ouvrir Outlook (sujet uniquement)

↓ Télécharger le modèle .eml

Modèle TAC 15 pour IOC Identified / Fixed Release disponible (WAVE 2a — Urgent Upgrade)

Scénario

Envoyé aux clients dont les journaux SD-WAN indiquaient **des indicateurs de compromission (IoC)** liés à CVE-2026-20245 ET pour lesquels une **version logicielle fixe est disponible**. Conseille au client de procéder à une mise à niveau urgente et de planifier un appel de révision pour discuter des conclusions et des mesures correctives.

Objet

URGENT : IoC identifié pour CVE-2026-20245 - Mise à niveau immédiate requise - SR [SR#]

Message

Cher client,

Nous vous remercions d'avoir contacté le centre d'assistance technique Cisco (TAC) pour le document CVE-2026-20245 dans la section Demande de service [SR#].

Après avoir analysé les fichiers admin-tech fournis par vos composants de contrôle SD-WAN, notre équipe a **identifié des indicateurs de compromission (IoC)** associés à CVE-2026-20245.

Compte tenu de la nature de ces résultats, il est essentiel que nous discutons des détails techniques et des prochaines étapes recommandées le plus tôt possible. Nous souhaiterions programmer un appel avec votre équipe pour passer en revue les résultats spécifiques et discuter du chemin de correction approprié.

Actions immédiates requises :

1. **Mise à niveau immédiate des composants de contrôle SD-WAN** : Une version logicielle fixe est disponible pour votre plate-forme. Veuillez mettre à niveau votre Manager (vManage), votre Controller (vSmart) et votre Validator (vBond) vers une version logicielle fixe répertoriée dans l'[avis de sécurité officiel](#)^[1] dès que possible. La mise à niveau ferme immédiatement la vulnérabilité.
2. **Planifier un appel de révision** : Faites-nous part de votre disponibilité pour un bref appel dans les prochaines [4 à 8 heures, par exemple] afin d'examiner les conclusions de l'IOC et de discuter des options de correction recommandées.
3. **Appliquer les meilleures pratiques de renforcement** : Examinez et mettez en oeuvre les recommandations du [Guide de sécurisation du SD-WAN de Cisco](#)^[2] afin de réduire votre surface d'attaque pendant que des mesures correctives sont prévues.

Ressources de mise à niveau :

- [Lancez la mise à niveau de votre Catalyst SD-WAN](#)^[3]
- [Guide de mise à niveau Cisco SD-WAN](#)^[4]

Important : Après la mise à niveau, des étapes de correction supplémentaires (telles que le redéploiement du contrôleur et la rotation du certificat) peuvent être recommandées en fonction de la gravité de la compromission identifiée. Ces points seront abordés au cours de l'appel de révision.

Reportez-vous également au [Guide de correction du TAC](#)^[5] pour obtenir des options de correction détaillées.

Notre objectif principal est de vous aider à sécuriser votre environnement et à limiter les risques potentiels. Nous apprécions votre prompt attention à cette question et nous nous réjouissons à l'idée de collaborer avec vous.

Cordialement,

Centre d'assistance technique Cisco (TAC)

Liens :

- [1] [Avis de sécurité officiel \(cisco-sa-sdwan-privesc-4uxFrzx\)](#)
- [2] [Guide de sécurisation du SD-WAN de Cisco](#)
- [3] [Commencez votre mise à niveau Catalyst SD-WAN](#)
- [4] [Guide de mise à niveau Cisco SD-WAN](#)
- [5] [Guide de correction TAC](#)

Ouvrir dans Outlook

① Remplacer tous les **[espaces réservés entre crochets]** avant l'envoi.

✉ Ouvrir Outlook (sujet uniquement)

⬇ Télécharger le modèle .eml

Modèle TAC 16 pour IOC identifié / Pas de version fixe disponible (WAVE 2a — durcissement et correction d'attente)

Scénario

Envoyé aux clients dont les journaux SD-WAN indiquaient **des indicateurs de compromission (IoC)** liés au CVE-2026-20245, mais pour lesquels **aucune version logicielle fixe n'est actuellement disponible** pour leur plate-forme/version. Recommande un durcissement immédiat, planifie un appel de révision et informe le client qu'il doit attendre que la version fixe soit entièrement corrigée.

Objet

URGENT : IoC identifié pour CVE-2026-20245 - Aucune version fixe actuellement disponible - SR [SR#]

Message

Cher client,

Nous vous remercions d'avoir contacté le centre d'assistance technique Cisco (TAC) pour le document CVE-2026-20245 dans la section Demande de service [SR#].

Après avoir analysé les fichiers admin-tech fournis par vos composants de contrôle SD-WAN, notre équipe a **identifié des indicateurs de compromission (IoC)** associés à CVE-2026-20245.

Compte tenu de la gravité de ces constatations, il est essentiel que nous discutons des détails techniques et que nous recommandions des mesures provisoires le plus tôt possible. Nous souhaiterions programmer un appel avec votre équipe afin de passer en revue les résultats spécifiques.

Important — Aucune Version De Logiciel Fixe Actuellement Disponible :

Pour le moment, **aucune version logicielle fixe n'est disponible** pour votre plate-forme et votre version logicielle actuelles afin de remédier entièrement à cette vulnérabilité. L'équipe d'ingénierie de Cisco travaille activement à fournir une version fixe. Une fois que le logiciel fixe sera disponible, l'[avis de sécurité officiel](#)^[1] sera mis à jour avec les informations de version fixe.

Actions immédiates requises :

1. **Planifier un appel de révision** : Faites-nous part de votre disponibilité pour un bref appel dans les prochaines [4 à 8 heures, par exemple] afin d'examiner les conclusions de l'IoC et de discuter des mesures de confinement provisoires.
2. **Appliquer Immédiatement Les Meilleures Pratiques De Renforcement** : Examinez et mettez en oeuvre les recommandations du [Guide de durcissement du SD-WAN de Cisco](#)^[2] afin de réduire votre surface d'attaque en attendant la version corrigée.
3. **Surveillance accrue** : Surveillez de près vos composants de contrôle SD-WAN pour détecter tout comportement anormal, toute modification de configuration inattendue ou toute tentative d'accès non autorisé.

4. **Surveiller les conseils de sécurité** : Consultez régulièrement l'[avis de sécurité officiel](#)^[1] pour obtenir des mises à jour sur la disponibilité des versions fixes de votre plate-forme.

5. **Planification de la mise à niveau** : Commencez dès maintenant la planification de la mise à niveau afin d'être prêt à exécuter la mise à niveau rapidement une fois la version corrigée publiée.

Étapes suivantes :

Nous mettrons à jour ce dossier lorsque la version logicielle fixe sera disponible. À ce stade, vous devez donner la priorité à la mise à niveau immédiate de tous les composants de contrôle SD-WAN (gestionnaire, contrôleur, validateur) vers la version fixe. Après la mise à niveau, des étapes de conversion supplémentaires (telles que le redéploiement du contrôleur et la rotation du certificat) seront abordées en fonction des résultats examinés au cours de notre appel.

Reportez-vous également au [Guide de correction du TAC](#)^[3] pour obtenir des informations sur les options de correction qui s'appliqueront une fois que la version fixe sera disponible.

Notre objectif principal est de vous aider à sécuriser votre environnement et à limiter les risques potentiels. Nous apprécions votre prompt attention à cette question et nous nous réjouissons à l'idée de collaborer avec vous.

Cordialement,

Centre d'assistance technique Cisco (TAC)

Liens :

[1] [Avis de sécurité officiel \(cisco-sa-sdwan-privesc-4uxFrdzx\)](#)

[2] [Guide de sécurisation du SD-WAN de Cisco](#)

[3] [Guide de correction TAC](#)

Ouvrir dans Outlook

① Remplacer tous les **[espaces réservés entre crochets]** avant l'envoi.

✉ Ouvrir Outlook (sujet uniquement)

⬇ Télécharger le modèle .eml

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.