

Remediate Catalyst SD-WAN Security Advisory - september 2026

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Overzicht van de herstelwerkstroom](#)

[Stap 1: Verzamel admin-tech bestanden van alle managers](#)

[Alternatief: handmatige verificatie \(alleen als de beheertechnologie niet kan worden verzameld\)](#)

[Stap 2: Upgrade naar een vaste softwareversie](#)

[Stap 3: Open een TAC-zaak en Upload Admin-Tech-bestanden voor het scannen](#)

[Stap 4: Als er een compromis wordt gevonden — TAC-richtsnoeren](#)

[Vaste softwareversies](#)

[Bijlage: Handmatige verificatiestappen \(alleen als het verzamelen van beheertechnologie niet mogelijk is\)](#)

[Hoe de indicatoren van compromis te identificeren](#)

[Verificatie 1: controleer het toegangslog voor de serviceproxy](#)

[Verificatie 2: controleer het serverlogboek van Manager](#)

[Veelgestelde vragen](#)

Inleiding

In dit document worden stappen beschreven om een kritieke SD-WAN-beveiligingslek te identificeren en op te lossen volgens de PSIRT-adviesdatums van 30 september 2026. Cisco raadt ten eerste aan om te upgraden naar een vaste softwarerelease om dit probleem op te lossen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Catalyst SD-WAN-architectuur en besturingscomponenten (Manager, Controller en Validator)
- Cisco Catalyst SD-WAN-upgradeprocedure

- Cisco TAC-casemanagement en procedures voor het verzamelen van beheertechnologie

Gebruikte componenten

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Voor gedetailleerde achtergrondinformatie en de laatste updates, zie de officiële PSIRT adviespagina.

Dit advies is beschikbaar via deze link:

- [Cisco Catalyst SD-WAN Manager API-verificatie omzeilt kwetsbaarheid](#) (CVE-2026-76504, CWE-177). Effectbeoordeling voor beveiliging: kritiek (CVSS-basiscore 9.8).

Dit defect wordt verholpen door dit PSIRT-advies:

- Cisco bug ID [CSCww79570](#)

Dit advies is van invloed op Cisco Catalyst SD-WAN Manager (vManage).

Overzicht van de herstelwerkstroom



Opmerking: alle SD-WAN-managers (vManage) die een release eerder uitvoeren dan de eerste vaste release zijn kwetsbaar en vereisen een onmiddellijke upgrade. Niet alle Catalyst Managers tonen echter bewijs van compromis.

Vereiste actie: Verzamel admin-techs van alle Catalyst SD-WAN Managers, upgrade alles naar een vaste release en open een Cisco TAC-case zodat TAC uw admin-techs kan scannen op indicatoren van compromis.

TAC is beschikbaar voor:

- Scan de admin-techs die u aanbiedt op indicatoren van compromis
- Upgradeondersteuning bieden als u problemen ondervindt tijdens de upgrade
- Begeleidt u door aanvullende remediëring als er compromisindicatoren worden geïdentificeerd

1. Verzamel admin-technieken - Voer admin-tech uit op alle Catalyst SD-WAN Managers,

inclusief elk knooppunt van een cluster en van een Disaster Recovery (DR)-implementatie, voorafgaand aan de upgrade om ervoor te zorgen dat er geen diagnostische gegevens verloren gaan. Selecteer Logboek- en technische opties. De kern is niet nodig.

2. Upgrade naar een vaste versie - Upgrade alle managers (vManage) naar een vaste softwareversie die wordt vermeld in de tabel met [vaste softwareversies](#).



Opmerking: wacht niet op TAC-scanresultaten voordat u een upgrade uitvoert. Upgraden naar een vaste release is de hoogste prioriteit en sluit de kwetsbaarheid. De TAC-scan in stap 3 bepaalt of er na de upgrade verdere actie nodig is.

3. Open een TAC-geval en upload Admin-Techs om te scannen op indicatoren van compromis
- Open een Cisco TAC-geval en upload alle admin-tech logbundels die zijn verzameld in stap 1. TAC scant de admin-techs op indicatoren van compromis.
4. Als er een compromis wordt gevonden, gebruikt u de TAC-richtlijn - Als de TAC indicatoren van een compromis in uw omgeving identificeert, vult u alle door de TAC verstrekte richtsnoeren voor herstel in. Als er geen compromisindicatoren worden gevonden, is er geen verdere actie nodig naast de upgrade.

Stap 1: Verzamel admin-tech bestanden van alle managers

Vereist: Verzamel admin-tech bestanden van alle Managers (vManage) voordat u een upgrade uitvoert om ervoor te zorgen dat er geen diagnostische gegevens verloren gaan. Deze bestanden worden door TAC in stap 3 gebruikt om uw omgeving te scannen op indicatoren van compromis.

Verzameling:



Opmerking: Voor het genereren van beheertechnologie selecteert u Logboek- en technische opties. De kern is niet nodig.

1. Voer admin-tech uit op ALL Managers (vManage).
2. Als uw managers als een cluster worden uitgevoerd, voert u op elk clusterlid admin-tech uit.
3. Als u een Disaster Recovery (DR)-implementatie hebt, voert u beheertechnologie uit op elke Manager in zowel de primaire als de DR-site.

[Verzamel een Admin-Tech in SD-WAN-omgeving en upload naar TAC-geval](#)



Opmerking: TAC analyseert deze bestanden om uw omgeving te beoordelen op indicatoren van compromis en het juiste herstelpad te begeleiden.

Alternatief: handmatige verificatie (alleen als de beheertechnologie niet kan worden verzameld)

Voor degenen die geen admin-tech-bestanden kunnen delen, zijn handmatige verificatiestappen beschikbaar. Deze stappen bieden voorlopige indicatoren die moeten worden gedocumenteerd en gedeeld met de TAC.

Zie het gedeelte [Handmatige verificatiestappen](#) aan het einde van dit document voor gedetailleerde procedures. Documenteer alle bevindingen en geef ze aan TAC in uw ondersteuningsgeval.

Stap 2: Upgrade naar een vaste softwareversie

Na het verzamelen van admin-techs in stap 1, upgrade alle Managers (vManage) naar een vaste softwareversie.



Belangrijk: wacht niet op de resultaten van de TAC-scan voordat u een upgrade uitvoert. Upgraden naar een vaste release is de hoogste prioriteit en sluit de kwetsbaarheid. De TAC-scan in stap 3 bepaalt of na de upgrade verdere actie nodig is.

Selecteer de juiste versie in de tabel [Vaste softwareversies](#) in dit document.



Waarschuwing: Upgrade moet binnen uw huidige belangrijke release blijven. Upgrade niet naar een hogere major release zonder expliciete TAC-richtlijnen.

[SD-WAN-controllers upgraden met vManage GUI of CLI](#)



Opmerking: Als u problemen ondervindt tijdens de upgrade, opent u een TAC-geval voor upgradeondersteuning.

Stap 3: Open een TAC-zaak en Upload Admin-Tech-bestanden voor het scannen

Na het upgraden in stap 2, opent u een Cisco TAC-ondersteuningscase en uploadt u de admin-tech-bestanden die in stap 1 zijn verzameld. TAC scant de admin-techs op indicatoren van compromis.

Vereiste acties:

1. Open een Severity 3 TAC-geval met de CVE-ID "CVE-2026-76504" in de titel om het scanproces te starten.
2. Upload ALLE bundels met beheertechnische logbestanden die zijn verzameld in stap 1 (alle managers, inclusief cluster- en DR-knooppunten).
3. Wacht tot de TAC de scan heeft voltooid en communiceer de resultaten.



Opmerking: TAC analyseert de admin-tech bestanden en communiceert de resultaten van de scan. Als er geen compromisindicatoren worden gevonden, is er geen verdere actie nodig naast de upgrade.

Stap 4: Als er een compromis wordt gevonden — TAC-richtsnoeren

Als TAC indicatoren van compromis in uw omgeving identificeert, neemt TAC contact met u op met specifieke saneringsrichtlijnen. Voltooi alle instructies van TAC.

Als er geen compromisindicatoren worden vastgesteld, is de in stap 2 voltooide upgrade voldoende en is er geen verdere correctie nodig.

Vaste softwareversies

Deze software releases bevatten de oplossing voor deze kwetsbaarheid. Upgrade naar de eerste vaste release in je huidige release-trein.

Cisco Catalyst SD-WAN Software Release	Eerste vaste release	Beschikbare software
Eerder dan 20,9 ¹	Migreren naar een vaste release.	
20.9	20.9.10.1	20.9.10.1 upgrade-images voor vManage
20.12	20.12.8.2	20.12.8.2 Upgradeimages voor vManage
20.15	20.15.6.1	20.15.6.1. Upgradeimages voor vManage

Cisco Catalyst SD-WAN Software Release	Eerste vaste release	Beschikbare software
20.18	20.18.4.1	20.18.4.1. Upgradeimages voor vManage
26.1	26.1.2.1	26.1.2.1. Upgradeimages voor vManage
26.2	26.2.1	26.2.1. Upgradeimages voor vManage

¹ Deze releases hebben het einde van het softwareonderhoud bereikt. Cisco moedigt klanten sterk aan om te upgraden naar een ondersteunde release.

Het Cisco Product Security Incident Response Team (PSIRT) valideert alleen de betreffende en vaste release-informatie die in het advies is gedocumenteerd.



Opmerking: Cisco heeft deze kwetsbaarheid ook aangepakt in Cisco SD-WAN Cloud (Cisco Managed) Release 20.15.605, die cloudgebaseerd is. Er is geen actie van de gebruiker vereist. Klanten kunnen de huidige herstelstatus of softwareversie bepalen met behulp van de Help-functie in de service-GUI.

Belangrijke referenties:

- [Upgradematrix](#)
- [Compatibiliteitsmatrix voor de controller](#)

Bijlage: Handmatige verificatiestappen (alleen als het verzamelen van beheertechnologie niet mogelijk is)



Opmerking: Admin-tech collectie is de voorkeur en aanbevolen methode. Gebruik alleen handmatige verificatie als u absoluut geen admin-tech-bestanden kunt verzamelen en delen. Als u geen admin-tech-bestanden kunt verzamelen, gebruikt u deze handmatige stappen om voorlopige indicatoren voor TAC te verzamelen.



Opmerking:

- Deze stappen bieden alleen voorlopige gegevens

- Admin-tech collectie heeft de voorkeur voor nauwkeurige beoordeling
- Documenteer uw bevindingen en deel ze met TAC in uw ondersteuningsgeval
- TAC maakt de officiële beoordeling

Vereisten: Deze stappen moeten worden uitgevoerd op alle managers (vManage), inclusief elk clusterlid en elke manager op een Disaster Recovery (DR)-site. Open de logbestanden van vshell (vshell van de CLI Manager) en bekijk zowel de huidige als de geroteerde logbestanden.

Hoe de indicatoren van compromis te identificeren

Dit advies heeft twee indicatoren van compromis. Beide hebben betrekking op items voor j_security_check waarin een teken van het verzoek is gecodeerd (bijvoorbeeld /%6a_security_check), van onbekende of niet-geautoriseerde IP-adressen.



Belangrijk: De voorbeelden in deze sectie tonen het gebruik van %6a als het gecodeerde teken j in het verzoek. Dit is slechts een voorbeeld, en de kwetsbaarheid staat toe dat elk teken dat in het verzoek is gecodeerd, wordt gebruikt.



Opmerking: Cisco Catalyst SD-WAN Manager-systemen die zijn blootgesteld aan het internet en die poorten hebben die zijn blootgesteld aan het internet, lopen het risico te worden blootgesteld aan compromissen. In sommige gevallen kunnen deze indicatoren van compromis optreden tijdens standaardbewerkingen. Daarom moeten ze worden beoordeeld aan de hand van de normale netwerkhouding om vals-positieven te identificeren en te vermijden.

aanwijzer	logbestand	Wat het betekent
Gecodeerde j_security_check-aanvraag ontvangen	/var/log/nms/containers/service_proxy/serviceproxy-access.log*	Een klant heeft een dergelijk verzoek naar de manager gestuurd.
Gecodeerde j_security_check aanvraag verwerkt voor een vptela-gereserveerde-* gebruiker	/var/log/nms/vmanage-server.log*	De beheerder heeft een dergelijk verzoek verwerkt voor een vptela-gereserveerde ** gebruiker (een gereserveerde systeemserviceaccount).

Verificatie 1: controleer het toegangslog voor de serviceproxy

Controleer het bestand `serviceproxy-access.log`, dat zich bevindt op `/var/log/nms/containers/service_proxy/serviceproxy-access.log`, op items die gerelateerd zijn aan `j_security_check` vanaf onbekende of niet-geautoriseerde IP-adressen, zoals in dit voorbeeld wordt getoond:

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

Bepaalde logbestanden in het vManage-systeem zijn beperkt achter de hoofdtoegang en kunnen niet rechtstreeks door klanten worden geopend. Om deze logs te bekijken, moeten klanten een admin-tech-bestand genereren.

Resultaten en document voor TAC interpreteren

Als dergelijke vermeldingen niet worden gevonden:

- Geen compromisindicatoren gevonden in dit log op deze Manager
- Documenteer dit resultaat voor uw TAC-geval
- Ga door met verificatie 2 en herhaal vervolgens beide verificaties voor de overige beheerders

Als dergelijke vermeldingen worden gevonden:

- Controleer zorgvuldig elk weergegeven bron-IP-adres
- Zoek naar vermeldingen van onbekende of niet-geautoriseerde IP-adressen. Controleer of het bron-IP-adres behoort tot een geautoriseerde activiteit in uw omgeving (bijvoorbeeld een kwetsbaarheidsscan of penetratietest die u uitvoert)
- Als u de bron-IP niet als legitiem kunt identificeren, kan dit wijzen op mogelijke indicatoren van compromis
- Documenteer alle bevindingen en open onmiddellijk een TAC-zaak
- Neem de loggegevens, tijdstempels, bron-IP's en HTTP-statuscodes in uw geval op
- TAC voert de officiële beoordelingsbepaling uit

Verificatie 2: controleer het serverlogboek van Manager

Controleer het bestand `vmanage-server.log`, dat zich bevindt op `/var/log/nms/vmanage-server.log`, op items die gerelateerd zijn aan `j_security_check` van onbekende of niet-geautoriseerde IP-adressen, specifiek opgeroepen voor gebruikers die namen bevatten die beginnen met `viptela-reserved-`, zoals in dit voorbeeld wordt getoond:

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



Opmerking: de voor vptela gereserveerde systeemserviceaccounts zijn gedocumenteerd in de sectie Authenticatie, autorisatie en boekhouding van de Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide.

Resultaten en document voor TAC interpreteren

Als dergelijke vermeldingen niet worden gevonden:

- Geen compromisindicatoren gevonden in dit log op deze Manager
- Documenteer dit resultaat voor uw TAC-geval
- Herhaal beide verificaties voor de overige managers

Als dergelijke vermeldingen worden gevonden:

- Dit kan wijzen op mogelijke indicatoren van een compromis
 - Documenteer alle bevindingen en open onmiddellijk een TAC-zaak
 - Neem de logboekvermeldingen en tijdstempels in uw geval op, samen met de bevindingen van Verificatie 1 voor dezelfde periode
 - TAC voert de officiële beoordelingsbepaling uit
-

Veelgestelde vragen

V: Wat is de eerste stap om dit beveiligingsadvies aan te pakken?

A: Verzamel admin-tech bestanden van alle Managers (vManage) en upgrade vervolgens alle Managers naar een vaste softwareversie. Open na het upgraden een TAC-geval en upload de admin-techs, zodat TAC uw omgeving kan scannen op indicatoren van compromis.

V: Welke onderdelen worden door dit advies beïnvloed?

A: Alleen Cisco Catalyst SD-WAN Manager (vManage) wordt beïnvloed.

V: Moeten we de controllers, validators of edge-routers ook upgraden?

A: Nee, niet om dit advies aan te pakken. Upgrade alle Managers (vManage) naar een vaste release en gebruik de [Controller Compatibility Matrix](#) om te bevestigen dat de nieuwe Manager-release compatibel is met uw andere componenten.

Q: Is er een workaround beschikbaar?

A: Nee. Er zijn geen workarounds die deze kwetsbaarheid aanpakken. Upgrade naar een vaste release.

V: Naar welke versie moet ik upgraden?

A: Upgrade zo snel mogelijk naar de eerste vaste release in je huidige release-trein. Raadpleeg de tabel [Vaste softwareversies](#) in dit document. TAC bevestigt de juiste versie voor uw specifieke

omgeving.

V: Ik heb al een upgrade uitgevoerd naar een vaste release voor een eerder SD-WAN-beveiligingsadvies. Moet ik opnieuw upgraden?

A: Ja, tenzij uw huidige release op of later is dan de eerste vaste release in uw trein in de tabel met [vaste softwareversies](#). Vaste releases voor eerdere adviezen bevatten niet noodzakelijkerwijs de oplossing voor deze kwetsbaarheid.

V: Moet ik admin-techs van alle managers verzamelen?

A: Ja. TAC vereist beheertechnische bestanden van elke Manager (vManage), inclusief elk clusterlid en elke Manager in een Disaster Recovery (DR) -site, om uw omgeving goed te beoordelen.

Q: Kan ik zelf controleren op indicatoren van compromis?

A: Ja. Als u geen beheertechnische bestanden kunt verzamelen, gebruikt u de [handmatige verificatiestappen](#) op elke manager en deelt u de resultaten met TAC. Admin-tech collectie blijft de voorkeursmethode, en TAC maakt de officiële beoordeling bepaling.

V: Hoe bepaalt TAC of mijn systeem is aangetast?

A: TAC analyseert de admin-tech bestanden met behulp van gespecialiseerde tools om uw omgeving te beoordelen op indicatoren van compromis.

V: Wat gebeurt er als er compromisindicatoren worden vastgesteld?

A: TAC neemt contact met u op om de volgende stappen en richtlijnen te bespreken die specifiek zijn voor uw omgeving. Cisco voert de sanering niet namens u uit - TAC biedt de nodige begeleiding om door te gaan.

V: Kan ik de upgrade starten voordat TAC mijn admin-techs analyseert?

A: Ja. Verzamel admin-techs, upgrade naar een vaste release en open vervolgens een TAC-geval zodat TAC de admin-techs kan scannen op indicatoren van compromis.

Q: Wordt downtime verwacht tijdens de sanering?

A: De impact hangt af van uw implementatiearchitectuur en het herstelpad. TAC biedt richtlijnen voor het minimaliseren van de impact op de dienstverlening tijdens het proces.

Q: Ik heb een cloud-hosted SD-WAN overlay. Wat zijn mijn opties voor upgraden?

A: Voor cloud-hosted overlays hebben klanten twee opties:

1. Controleer of uw omgeving is gepland voor een geautomatiseerde upgrade door te navigeren naar SSP > Overlay Details > Windows wijzigen.
2. Als u niet wilt wachten op de geplande upgrade, hebt u twee opties:
 - Upgrade zelfstandig met behulp van de upgradehulplijnen die in dit document

beschikbaar zijn.

- Open een stand-by TAC-hoesje voor het onderhoudsvenster van uw voorkeur. TAC is beschikbaar om u te helpen als u problemen ondervindt met de upgrade.

Q: Wij zijn een Cisco-gehoste overlay. Moeten we de toegangsregels voor SSP herzien?

A: Alle door Cisco gehoste klanten wordt geadviseerd om hun eigen Toegestane Inkomende Regels in SSP > Overlay Details > Toestaan Inkomende regels en zorg ervoor dat alleen de nodige voorvoegsels van uw kant zijn toegestaan. Deze regels gelden alleen voor beheerstoegang en niet voor edge-routers.

V: Biedt Cisco TAC forensische analyse- of onderzoeksdiensten voor deze kwetsbaarheid?

A: Cisco TAC kan klanten helpen door te scannen op indicatoren van compromis (IoC's) met betrekking tot deze kwetsbaarheid. TAC voert echter geen diepgaande forensische analyse of incidentonderzoeken uit. Voor uitgebreid forensisch werk of gedetailleerde beveiligingsonderzoeken raden we klanten aan om hun voorkeursbedrijf voor incidentrespons (IR) van derden in te schakelen.

V: Wat zijn de algemene best practices of manieren om kwetsbaarheden voor mijn SD-WAN-overlay te verminderen?

Raadpleeg de [Cisco Catalyst SD-WAN Hardening Guide](#) voor best practices en aanbevelingen om kwetsbaarheden in uw SD-WAN-overlay te verminderen.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.