Remediate Catalyst SD-WAN Security Advisory - jun 2026

Inhoud

Inleiding

Dit document beschrijft stappen om kritieke beveiligingslekken in SD-WAN te identificeren en aan te pakken op basis van PSIRT-adviezen van 4 juni 2026.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Catalyst SD-WAN-architectuur en besturingscomponenten (vManage, vSmart, vBond)
- Cisco Catalyst SD-WAN-upgradeprocedure
- Cisco TAC-casemanagement en procedures voor het verzamelen van beheerderstechnologie

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, raadpleegt u de officiële PSIRT-adviespagina.

Deze adviezen zijn beschikbaar via deze links:

- Cisco Catalyst SD-WAN Manager Authenticated Privilege Escalation Vulnerability

Deze gebreken worden behandeld door deze PSIRT-adviezen:

- Cisco bug ID CSCwu18563

Overzicht van de werkstroom voor probleemoplossing

Dit advies beschrijft een kwetsbaarheid voor privilege-escalatie in SD-WAN Manager waarvoor netadmin-bevoegdheden nodig zijn om te kunnen exploiteren.

Volgens het advies zijn de bekende paden voor een niet-geverifieerde externe aanvaller om die bevoegdheden te verkrijgen, exploitatie van CVE-2026-20182 (cisco-sa-sdwan-rpa2-v69WY2SW) of CVE-2026-20127 (cisco-sa-sdwan-rpa-EHchtZk).

Als uw besturingscomponenten zijn geüpgraded naar een vaste release voor beide adviezen en Cisco geen potentiële indicatoren van compromis (IoC's) heeft geïdentificeerd in de admin-tech-bestanden die u voor de eerdere gebeurtenissen hebt verstrekt, worden de bekende niet-geverifieerde exploitatiepaden voor deze nieuwe kwetsbaarheid beperkt op die specifieke apparaten, op basis van de beoordeelde bestanden.

Dit elimineert de blootstelling niet wanneer een aanvaller geldige netadmin-referenties heeft. Cisco heeft nog geen software-oplossing voor dit beveiligingslek vrijgegeven en er zijn geen oplossingen beschikbaar; verdere richtlijnen zullen volgen zodra deze beschikbaar komt.

Vereiste actie: Open een Cisco TAC-case om dit beveiligingsadvies aan te pakken.

De TAC is beschikbaar voor:

- Beoordeel uw omgeving op indicatoren van compromis

- Begeleid u door het juiste herstelpad op basis van de beoordeling
- Begeleiding geven over de volgende stappen die moeten worden genomen als er compromisindicatoren worden vastgesteld

1. Verzamel Admin-Techs- Voer admin-tech uit op alle besturingscomponenten (vSmart, vManage, vBond). vSmart-beheertechnologieën mogen niet gelijktijdig worden uitgevoerd — voer ze één voor één uit. Alle andere kunnen in elke volgorde worden verzameld. Selecteer Logboekopties en Technische opties. De kern is niet nodig.
2. Open TAC Case - Neem contact op met Cisco TAC en zorg voor alle logbundels van Control Component Admin-tech.
3. TAC-beoordeling - Voer een voorlopige beoordeling uit van de indicatoren van compromis binnen uw omgeving en TAC voert een voorlopige beoordeling uit van de indicatoren van compromis in uw omgeving.
4. Remediation uitvoeren - Voltooi indien nodig het specifieke proces dat door TAC wordt geboden.

Stap 1: Verzamel Admin-Tech-bestanden van alle besturingscomponenten

Vereist: Verzamel admin-tech bestanden van alle besturingscomponenten voordat u een upgrade of configuratiewijziging uitvoert, zodat diagnostische gegevens en mogelijke indicatoren van compromis (IoC's) behouden blijven. Deze bestanden worden door TAC in stap 3 gebruikt om uw omgeving te analyseren.

Collectie: Selecteer Logboekopties en technische opties voor het genereren van beheerderstechnologie. De kern is niet nodig.

1. Voer admin-tech uit op ALLE controllers (vSmarts) - voer deze niet tegelijkertijd uit; verzamel er één tegelijk
2. Voer admin-tech uit op ALLE managers (vManages)
3. Voer admin-tech uit op ALLE validators (vBonds)

Verzamel een Admin-Tech in SD-WAN-omgeving en upload naar TAC Case

---

Opmerking: TAC analyseert deze bestanden om uw omgeving te beoordelen op compromisindicatoren met betrekking tot dit advies. De analyse voor dit advies is gericht op een specifieke logboekregistratie waarbij geen onderscheid wordt gemaakt tussen legitiem en kwaadwillig gebruik; handmatige controle door TAC is vereist.

Alternatief: Handmatige verificatie (alleen als Admin-Tech niet kan worden verzameld)

Voor klanten die geen admin-tech-bestanden kunnen delen, is een handmatige verificatiestap

beschikbaar. Deze stap biedt een voorlopige indicator die moet worden gedocumenteerd en gedeeld met de TAC.

Zie het gedeelte Handmatige verificatiestappen aan het einde van dit document voor een gedetailleerde procedure. Documenteer alle bevindingen en geef ze aan TAC in uw ondersteuningsgeval.

Stap 2: Open een TAC Case en upload Admin-Tech Files

Nadat u admin-techs hebt verzameld in stap 1, opent u een ondersteuningscase voor Cisco TAC en uploadt u de verzamelde admin-techbestanden. TAC analyseert de admin-techs voor compromisindicatoren die verband houden met dit advies.

Vereiste acties:

1. Open een TAC-geval voor prioriteitsniveau 3 met "CVE-2026-20245" en de adviserende ID `cisco-sa-sdwan-privesc-4uxFredzx` in de titel om de analyse te starten.
2. Upload ALLE logboekbundels voor beheerderstechnologie die in stap 1 zijn verzameld (controllers, beheerders en validators).
3. Wacht tot TAC de analyse heeft voltooid en de resultaten heeft meegedeeld.

Opmerking: Cisco heeft geen softwarefix voor dit beveiligingslek uitgebracht en er zijn geen oplossingen beschikbaar. De TAC-analyse in stap 3 helpt te bepalen of er compromisindicatoren aanwezig zijn in de door u verstrekte admin-tech-bestanden. Verdere richtlijnen zullen volgen als het beschikbaar komt van engineering.

Stap 3: TAC-beoordeling

TAC voert een voorlopige analyse uit van de admin-tech-bestanden die u in stap 2 hebt geüpload en beoordeelt deze op compromisindicatoren die aan dit advies zijn gekoppeld.

Voor dit advies is de analyse gericht op een specifieke logboekvermelding in `/var/log/scripts.log` op elke Manager (vManage). Omdat de onderliggende opdracht legitiem is en het logboek geen onderscheid maakt tussen legitiem en kwaadwillig gebruik, vereisen alle overeenkomende items handmatige beoordeling door TAC tegen de normale operationele houding van de klant voordat ze worden behandeld als een bevestigde indicator.

Mogelijke uitkomsten van de TAC-analyse:

- Er werden geen overeenkomende logboekvermeldingen geïdentificeerd — op basis van de beoordeelde admin-tech-bestanden werden geen indicatoren in verband met dit advies waargenomen. Op dit moment is geen specifieke actie voor dit advies vereist. Het resultaat is beperkt tot de ontvangen admin-tech-bestanden en kan worden beperkt door de

bewaarperiode voor logbestanden op elk apparaat.
- Overeenkomende logboekgegevens geïdentificeerd — TAC zal de klant betrekken bij aanvullende controlestappen. Omdat Cisco geen softwarefix voor dit advies heeft uitgebracht, lost de upgrade alleen dit beveiligingslek niet op. De richtlijnen van TAC voor bevestigde compromisscenario's zijn gedocumenteerd in de gerelateerde TechZone-artikelen waarnaar wordt verwezen in stap 4.

Opmerking: volgens het advies vereist de exploitatie van dit beveiligingslek netadmin-bevoegdheden, die een niet-geverifieerde aanvaller alleen kan verkrijgen via geldige referenties of exploitatie van CVE-2026-20182 of CVE-2026-20127. Als uw besturingscomponenten zijn geüpgraded naar een vaste release voor beide adviezen en er geen compromisindicatoren zijn geïdentificeerd voor de eerdere gebeurtenissen, worden de bekende niet-geverifieerde exploitatiepaden voor deze nieuwe kwetsbaarheid beperkt op die specifieke apparaten, op basis van de beoordeelde bestanden.

Stap 4: Als er compromisindicatoren worden vastgesteld — Volg de TAC-richtsnoeren

Als TAC compromisindicatoren identificeert die verband houden met dit advies in uw omgeving, neemt TAC contact met u op met specifieke richtlijnen. Vul alle instructies in die door TAC worden verstrekt.

Als er geen compromisindicatoren zijn vastgesteld voor dit advies, is op dit moment geen verdere specifieke actie voor dit advies vereist, op basis van de bestudeerde admin-tech-bestanden.

Belangrijk: Cisco heeft geen softwarefix voor dit advies uitgebracht en er zijn geen oplossingen beschikbaar. Omdat voor het exploiteren van deze kwetsbaarheid netadmin-bevoegdheden vereist zijn die zijn verkregen via CVE-2026-20182 of CVE-2026-20127, moeten klanten ervoor zorgen dat deze eerdere adviezen volledig zijn verholpen. Raadpleeg de bijbehorende documenten voor de vastgestelde herstelstroom:

---

overwegingen

Aan het einde van een succesvolle sanering en op basis van de specifieke eisen van elke klant voor de beveiliging, willen klanten mogelijk de volgende hygiëneactiviteiten evalueren en uitvoeren. Deze activiteiten zijn van toepassing ongeacht welke hersteloptie is geselecteerd. Ze worden door de klant beheerd; Cisco leidt of voert ze niet uit namens de klant.

- Controle van alle lokale gebruikersaccounts

- Rotatie van referenties
- Rotatie van eventuele geheimen in apparaatconfiguraties, bijvoorbeeld (niet-uitputtende lijst):
  - Inloggegevens voor lokale gebruikersaccounts
  - SNMP-communitystrings
  - TACACS geheime sleutels
  - VPN vooraf gedeelde sleutels en certificaten
  - Vertrouwde SSH-sleutels
- Controle van configuratiesjablonen

Randapparatuur — Vermoede compromittering

Cisco raadt een bepaald saneringspad niet aan; de keuze van een saneringsoptie berust bij de klant. Als informatieve opmerking voor klanten die hun omgeving evalueren: wanneer de klant vermoedt dat een randapparaat in gevaar is, is een fabrieksreset en het opnieuw instappen van de getroffen randapparaten een door de klant beheerde actie waarmee de klant mogelijk rekening wil houden bij het maken van zijn selectie. De beslissing om deze aanpak te volgen en welke optie te selecteren, ligt bij de klant.

De juiste opdracht voor het uitvoeren van een veilige fabrieksreset is:

```
factory-reset all secure 3-pass
```

Vaste softwareversies

⚠ Belangrijk: op het moment van publicatie van dit document heeft Cisco geen softwarefix vrijgegeven die CVE-2026-20245 adresseert. Volgens het advies is Cisco van plan om deze kwetsbaarheid in Cisco Catalyst SD-WAN Manager in een toekomstige release aan te pakken. Er zijn geen workarounds. Deze sectie wordt bijgewerkt wanneer vaste software beschikbaar komt.

Omdat voor de exploitatie van deze kwetsbaarheid netadmin-bevoegdheden vereist zijn die een niet-geverifieerde aanvaller alleen via CVE-2026-20182 of CVE-2026-20127 kan verkrijgen, worden klanten aangemoedigd ervoor te zorgen dat hun besturingscomponenten een vaste release voor die eerdere adviezen uitvoeren. De vaste releases voor die adviezen zijn gedocumenteerd in de SD-WAN Security Advisory van 14 mei 2026 en het bijbehorende TechZone-document:

- Cisco Catalyst SD-WAN Controller Authentication Bypass Vulnerability (14 mei 2026)
- (tabel met vaste softwareversies)

Belangrijke referenties:

- Upgradematrix
- compatibiliteitsmatrix voor controllers

Bijlage: Handmatige verificatiestappen (alleen als Admin-Tech Collection niet mogelijk is)

Opmerking: Admin-tech-verzameling is de voorkeursmethode. Gebruik de onderstaande handmatige verificatiestap alleen als er geen admin-tech-bestanden kunnen worden verzameld en gedeeld met TAC. Het resultaat van deze handmatige stap is voorlopig; documenteer bevindingen en deel ze met TAC, die de officiële beoordeling uitvoert.

Opmerking: voor dit advies bestaat de handmatige verificatie uit één gerichte logboekcontrole. Het opgezochte logboekitem wordt gegenereerd door een legitieme opdracht en het logboek alleen maakt geen onderscheid tussen legitiem en kwaadwillig gebruik. Elke overeenkomende vermelding moet worden beoordeeld aan de hand van de normale operationele houding van de klant voordat deze als een potentiële indicator wordt behandeld. Als een overeenkomende vermelding niet kan worden aangesloten op normale activiteiten, documenteert u de bevinding en deelt u deze met TAC.

Verificatie: controleer `scripts.log` op elke Manager (vManage) voor Uploadvermeldingen van de lijst met huurders

Volgens het PSIRT-advies worden klanten aangemoedigd om het bestand `scripts.log`, dat zich bevindt op `/var/log/`, te controleren voor vermeldingen die vergelijkbaar zijn met het volgende voorbeeld:

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

Stap 1: Open vshell op elke Manager (vManage) en zoek het logbestand

Ga vanuit de vManage CLI naar vshell en voer het volgende uit:

```
vs
zgrep "vconfd_script_upload_tenant_list.sh" /var/log/scripts.log*
```

Herhaal de controle op elke vManage-server in de implementatie (inclusief alle clusterleden en alle aan DR gekoppelde vManage).

Stap 2: Interpreteren van resultaten en documenten voor TAC

Als er GEEN overeenkomende items worden geretourneerd:

- In het logbestand van dit apparaat zijn geen compromisindicatoren in verband met dit advies waargenomen.
- Documenteer dit resultaat voor uw TAC-geval (vermeld de hostnaam van het apparaat en de datum/het bereik van de gezochte logbestanden).
- Ga verder met het controleren van de resterende managers.

Als overeenkomende items worden teruggegeven:

- Elke overeenkomende vermelding moet worden beoordeeld aan de hand van de normale operationele houding van de klant. De onderliggende opdracht (upload van de lijst met huurders) is legitiem en kan tijdens routinebewerkingen worden weergegeven.
- Leg voor elk overeenkomend item de tijdstempel, de volledige logregel en het bestandspad vast waarnaar wordt verwezen na het `cli-pad`.
- Als een overeenkomende vermelding niet kan worden verzoend met een bekende, legitieme bewerking, kan dit een indicatie van compromis zijn. Documenteer de bevinding en geef deze aan TAC voor herziening.
- Documenteer alle bevindingen en open een TAC-zaak. Voeg de overeenkomende logboekvermeldingen en de uitvoer van de bronopdracht in uw geval toe.
- TAC voert de officiële beoordeling uit. Als de beoordeling compromisindicatoren identificeert, volgt u de stroom die wordt beschreven in de gerelateerde TechZone-documenten: en handleidingen voor probleemoplossing.

Veelgestelde vragen

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

A: Verzamel admin-tech-bestanden van alle besturingscomponenten (vSmart, vManage, vBond) voordat u een upgrade of configuratiewijziging uitvoert om diagnostische gegevens en eventuele compromisindicatoren te behouden. Open vervolgens een Cisco TAC-case en upload de admin-techs zodat TAC ze kan analyseren.

V: Heeft Cisco een softwarefix uitgebracht voor deze kwetsbaarheid?

A: Niet op het moment van publicatie van dit document. Volgens het advies is Cisco van plan om deze kwetsbaarheid in Cisco Catalyst SD-WAN Manager in een toekomstige release aan te pakken. Er zijn geen workarounds. Dit document wordt bijgewerkt wanneer een vaste release beschikbaar komt.

V: Als er geen oplossing is, waarom beveelt Cisco dan nu actie aan?

A: Het gebruik van deze kwetsbaarheid vereist netadmin privileges. Volgens het advies kan een niet-geverifieerde aanvaller die bevoegdheden alleen verkrijgen via geldige referenties of door gebruik te maken van CVE-2026-20182 of CVE-2026-20127. Ervoor zorgen dat besturingscomponenten worden geüpgraded naar de vaste releases voor die eerdere adviezen, richt zich op de bekende niet-geverifieerde paden om de bevoegdheden te verkrijgen die nodig zijn om deze kwetsbaarheid te exploiteren. De admin-tech-analyse in stap 3 helpt bepalen of er compromisindicatoren aanwezig zijn in de beoordeelde bestanden.

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

A: Ja. TAC vereist admin-tech-bestanden van alle controllers (vSmart, één voor één verzameld), alle managers (vManage) en alle validators (vBond) om de analyse uit te voeren.

V: Hoe bepaalt TAC of mijn systeem compromisindicatoren heeft in verband met dit advies?

A: TAC beoordeelt de admin-tech bestanden en zoekt naar de specifieke log entry beschreven in de PSIRT advies in `/var/log/scripts.log` op elke Manager. De onderliggende opdracht is legitiem; elke overeenkomende invoer moet worden beoordeeld aan de hand van uw normale operationele houding voordat deze als een potentiële indicator wordt behandeld. TAC voert deze beoordeling uit.

V: Wat gebeurt er als er compromisindicatoren worden vastgesteld?

A: TAC neemt contact met u op met specifieke begeleiding. Omdat er momenteel geen softwarefix beschikbaar is voor dit advies, lost de upgrade alleen een bevestigd compromis niet op. De richtlijnen van TAC volgen de stroom gedocumenteerd in de gerelateerde TechZone-artikelen voor de adviezen van mei 2026 en februari 2026.

V: Worden edge routers (Cisco IOS XE) beïnvloed door dit advies?

A: Dit advies is van invloed op Cisco Catalyst SD-WAN Manager. Volgens het advies heeft Cisco beperkte gevallen waargenomen waarin exploitatie van dit beveiligingslek resulteerde in een configuratiewijziging die naar edge-apparaten werd gepusht; klanten worden aangemoedigd om de configuratie van hun edge-apparaten te verifiëren.

V: Welke implementatietypen worden beïnvloed?

A: Volgens het advies heeft dit beveiligingslek gevolgen voor alle implementatietypen van Cisco Catalyst SD-WAN Manager, ongeacht de apparaatconfiguratie, waaronder On-Prem Deployment, Cisco SD-WAN Cloud-Pro, Cisco SD-WAN Cloud (Cisco Managed) en Cisco SD-WAN for Government (FedRAMP).

V: Ik heb al een upgrade uitgevoerd voor de adviezen van mei 2026 en februari 2026 en er zijn voor die evenementen geen compromisindicatoren vastgesteld. Sta ik bloot aan deze nieuwe kwetsbaarheid?

A: Als uw besturingscomponenten een vaste release hebben voor zowel CVE-2026-20182 als CVE-2026-20127 en er geen compromisindicatoren zijn geïdentificeerd voor die eerdere gebeurtenissen in de beoordeelde admin-tech-bestanden, worden de bekende niet-geverifieerde

exploitatiepaden voor deze nieuwe kwetsbaarheid beperkt op die specifieke apparaten, op basis van de beoordeelde bestanden. Dit elimineert blootstelling niet wanneer een aanvaller geldige netadmin referenties heeft.

V: Kan ik de verificatie zelf uitvoeren in plaats van te wachten op TAC?

A: Klanten die geen beheerderstechnieken kunnen delen, kunnen de handmatige verificatiestap uitvoeren die in de bijlage wordt beschreven. Het resultaat is voorlopig; documenteer bevindingen en deel ze met TAC, die de officiële beoordeling uitvoert.

V: Wat zijn de algemene best practices voor het verharden van mijn SD-WAN-overlay?

A: Raadpleeg de Cisco Catalyst SD-WAN Hardening Guide voor best practices.

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

A: Cisco TAC kan klanten helpen door admin-tech-bestanden te bekijken voor de compromisindicatoren die zijn gedocumenteerd in het PSIRT-advies. Cisco TAC voert geen diepgaande forensische analyse of incidentonderzoek uit. Voor uitgebreid forensisch werk of gedetailleerde veiligheidsonderzoeken worden klanten aangemoedigd om hun favoriete derde partij Incident Response (IR)-bedrijf in te schakelen.

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.