# Remediate Catalyst SD-WAN Security Advisory - februari 2026

## Inhoud



## Inleiding

Dit document beschrijft stappen om kritieke beveiligingslekken in SD-WAN te identificeren en op te lossen op basis van PSIRT-adviezen van 25 februari 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-kwetsbaarheden
- Cisco Catalyst SD-WAN-controllerverificatie omzeilt kwetsbaarheid

Deze gebreken worden behandeld door deze PSIRT-adviezen:

- Cisco bug ID CSCws52722
- Cisco bug ID CSCws33583
- Cisco bug ID CSCws33584
- Cisco bug ID CSCws33585
- Cisco bug ID CSCws33586
- Cisco bug ID CSCws33587
- Cisco bug ID CSCws93470

---

## Overzicht van de werkstroom voor probleemoplossing

---

Opmerking: alle SD-WAN-implementaties zijn kwetsbaar en vereisen onmiddellijke actie. Niet alle systemen vertonen echter tekenen van compromis.

---

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
- Werk samen met het PSIRT-team als er compromisindicatoren worden vastgesteld
- Upgradebegeleiding en -ondersteuning bieden als er geen compromisindicatoren worden gedetecteerd

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 - TAC beoordeelt uw omgeving voor compromisindicatoren
4. Herstel uitvoeren - Voltooi 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 uw TAC-case opent. Dit is essentieel voor TAC om uw omgeving te beoordelen.

Verzameling:

---

Opmerking: 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)

---

Opmerking: vSmart admin-techs mogen niet gelijktijdig worden uitgevoerd — verzamel ze één voor één. Admin-techs voor Managers en Validators kunnen in elke volgorde worden verzameld.

---

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 en het juiste herstelpad te begeleiden.

---

### Alternatief: Handmatige verificatie (alleen als Admin-Tech 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 de sectie "Handmatige verificatiestappen" aan het einde van dit document voor gedetailleerde procedures. Documenteer alle bevindingen en geef ze aan TAC in uw ondersteuningsgeval.

---

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

Nadat u alle admin-tech-bestanden van stap 1 hebt verzameld, opent u een ondersteuningscase voor Cisco TAC.

Vereiste acties:

1. Open een TAC-geval met een prioriteitsniveau dat geschikt is voor uw zakelijke impact
2. Upload ALLE logboekbundels voor beheerderstechnologie die in stap 1 zijn verzameld (controllers, beheerders en validators)
3. Raadpleeg de PSIRT-adviezen
4. Wachten op TAC-beoordeling en -richtsnoeren

---

⚠ Let op: TAC bepaalt de status van uw systeem en beveelt passende volgende stappen aan.

Probeer geen verdere stappen zonder TAC-richtsnoeren

---

## Stap 3: TAC-beoordeling

TAC analyseert de geüploade admin-tech bestanden en bepaalt de status van uw systeem.

Gedurende deze tijd:

- Wacht op een officiële beoordeling van de TAC voordat u actie onderneemt
- TAC neemt contact met u op met hun bevindingen en volgende stappen

---

## Stap 4: Remediation uitvoeren (TAC-geleid)

TAC begeleidt u door het juiste herstelproces op basis van hun beoordeling. Vul alle instructies in die door TAC worden verstrekt.

### Pad A: geen compromisindicatoren gevonden — upgrade

Als TAC bevestigt dat er geen bewijs is van een compromis, upgrade dan naar de vaste

softwareversie. Selecteer de juiste versie in de tabel Vaste softwareversies in dit document en raadpleeg de upgradehandleiding die in deze sectie is gekoppeld.

---

Waarschuwing: de upgrade moet binnen de huidige hoofdrelease blijven. Niet upgraden naar een hogere belangrijke release zonder expliciete TAC-richtlijnen.

---

Upgrade SD-WAN-controllers met behulp van vManage GUI of CLI

### Pad B: geïdentificeerde compromisindicatoren — PSIRT-geleid

Als TAC bevestigt dat er compromisindicatoren aanwezig zijn, schakelen ze het PSIRT-team in om een aangepaste saneringsstrategie te ontwikkelen die specifiek is voor uw omgeving. Vul alle richtlijnen aan die door TAC en PSIRT worden verstrekt.

---

## Vaste softwareversies

Deze softwarereleases bevatten oplossingen voor de geïdentificeerde kwetsbaarheden:

| Geldt voor huidige versies | Vaste versie | Beschikbare software |
|---|---|---|
| 20,3, 20,6, 20,9 | 20.9.8.2 * | 20.9.8.2 Upgrade-images voor vManage, vSmart en vBond |
| 20 .10, 20 .11, 20.12.5 en eerder in 30 .12 | 20.12.5.3 | 20.12.5.3 Upgrade-images voor vManage, vSmart en vBond |
| 20.12.6 | 20.12.6.1 | 20.12.6.1 Upgrade-images voor vManage, vSmart en vBond |
| 20,13, 20,14, 20,15,x | 20.15.4.2 | 20.15.4.2 Upgrade-images voor vManage, vSmart en vBond |
| 20,16, 20,17, 20,18,x | 20.18.2.1 | 20.18.2.1 Upgrade-images voor vManage, vSmart en vBond |

---

Opmerking: voor klanten op CDCS (Cisco-Hosted Cluster) is 20.15.405 ook een vaste release. Dit is specifiek van toepassing op de door Cisco gehoste clusterimplementatie en wordt afzonderlijk van het standaard upgradepad behandeld.

---

* Als u op release 20.9 of eerder: De vaste software voor uw release (20.9.8.2) is beschikbaar op

2/27. Cisco raadt aan om binnen uw huidige hoofdrelease te blijven en te wachten op de 20.9.8.2-release in plaats van te upgraden naar een hogere hoofdrelease (20 .12, 20.15, 20.18). Als u momenteel in een versie lager dan 20.9 bent, wacht dan tot 20.9.8.2 om daar te upgraden. Blijf werken met TAC en controleer 2/27 voor de beschikbare softwarelink.

Belangrijke referenties:

- Upgrade matrix
- compatibiliteitsmatrix voor controllers

---

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

---

Opmerking: Admin-tech-verzameling is de voorkeursmethode 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 leveren alleen voorlopige gegevens op
- Admin-tech-verzameling heeft sterk de voorkeur voor nauwkeurige beoordeling
- Documenteer uw bevindingen en deel ze met TAC in uw ondersteuningsgeval
- TAC bepaalt de officiële beoordeling

---

Vereisten: Deze stappen moeten worden uitgevoerd op alle besturingscomponenten.

## Verificatie 1: controleren op ongeautoriseerde SSH-aanmeldingen in Auth-logboeken

Stap 1: Identificeer geldige vManage-systeem-IP's

Toegang tot elke vSmart-controller en uitvoering:

```
west-vsmart# show control connections | inc "vmanage|PEER|IP"
```

Voorbeeld van uitvoer:

```
                                                  PEER
      PEER  PEER  PEER            SITE       DOMAIN  PRIV    PEER                                    PUB
INDEX TYPE  PROT  SYSTEM IP       ID         ID      PRIVATE IP                              PORT    PUBLIC I
-----------------------------------------------------------------------------------------------------------
0     vmanage dtls 10.1.0.18     101018     0       10.1.10.18                              12346   10.1.10.1
```

Stap 2: Reguliere expressiereeks maken (alleen vBond en vSmart)

Combineer alle systeem-IP's van stap 1 in een OR-regex-patroon:

```
system-ip1|system-ip2|...|system-ipn
```

Stap 2b: Extra stap voor vManage-systemen

Als u deze opdrachten op vManage zelf uitvoert, voegt u de IP van de localhost (127.0.0.1), de IP van het lokale systeem, alle cluster-IP's en de IP van de VPN 0-transportinterface toe aan de regex:

```
system-ip1|system-ip2|...|system-ipn|127.0.0.1|
```

Als u het lokale IP-adres van het vManage-systeem wilt vinden, gebruikt u:

```
show control local-properties
```

Om de VPN 0-transportinterface IP en cluster IP te vinden, gebruikt u:

```
show interface | tab
```

Stap 3: Verificatie uitvoeren, opdracht

Voer deze opdracht uit en vervang REGEX door uw regex-tekenreeks uit stap 2:

```
west-vsmart# vs
```

```
west-vsmart:~$ zgrep "Accepted publickey for vmanage-admin from " /var/log/auth.log* | grep -vE "\s(REG
```

---

Opmerking: met deze opdracht worden verificatielogboeken gefilterd zodat alleen aanmeldingen van vmanage-admin uit onverwachte bronnen worden weergegeven. Legitieme aanmeldingen mogen alleen afkomstig zijn van aan vManage gerelateerde IP's.

---

Stap 4: Resultaten en document voor TAC interpreteren

Als GEEN uitvoer wordt weergegeven:

- Er zijn geen compromisindicatoren gedetecteerd op dit apparaat
- Documenteer dit resultaat voor uw TAC-geval
- Doorgaan met beoordeling van resterende controllers

Als logboeklijnen worden afgedrukt:

- Controleer zorgvuldig elk weergegeven IP-adres
- Controleer of het IP-adres niet gerelateerd is aan de vManage-infrastructuur (cluster-IP, oude systeem-IP of vergelijkbaar)
- Als u de bron-IP niet als legitiem kunt identificeren, kan dit wijzen op potentiële indicatoren van compromis
- De logboekvermelding toont een tijdstempel en een bron-IP-adres
- Documenteer alle bevindingen en open onmiddellijk een TAC-zaak
- Voeg de logboekvermeldingen, tijdstempels en bron-IP's in uw geval toe
- TAC voert de officiële beoordelingsbepaling uit

## Verificatie 2: Controleren op ongeautoriseerde peer-verbindingen in controllersystemen

Deze opdracht extraheert alle peer-type en peer-systeem-ip-paren van controller syslog-bestanden en voert ze uit als een lijst die u kunt bekijken. Het markeert niet automatisch verdachte vermeldingen - u moet de uitvoer inspecteren en bepalen of elk peer-IP-systeem een bekend, legitiem onderdeel van uw SD-WAN-infrastructuur is. Voer dit uit op alle besturingscomponenten (controllers, beheerders en validators).

Stap 1: Voer de opdracht uit op elke besturingscomponent:

Ga eerst naar vshell en navigeer naar de logdirectory:

```
vs
cd /var/log
```

Voer vervolgens de volgende opdracht uit:

```
awk '{
  match($0, /peer-type:([a-zA-Z0-9]+)[^ ]* peer-system-ip:([0-9.:]+)/, arr);
  if(arr[1] && arr[2]) print "(" arr[1] ", " arr[2] ")";
}' vsyslog* | sort | uniq
```

Stap 2: Interpreteren van resultaten en documenten voor TAC

Als uit de uitvoer alleen bekende IP's van het vManage/vSmart/vBond-systeem worden weergegeven:

- Bij deze controle werden geen compromisindicatoren ontdekt
- Documenteer dit resultaat voor uw TAC-geval
- Doorgaan met de beoordeling van resterende besturingscomponenten

Als uitvoer niet-herkende IP's van het peer-systeem bevat:

- Bekijk zorgvuldig elk IP-adres en peer-type dat wordt weergegeven
- Controleer of het IP-adres niet gerelateerd is aan uw bekende SD-WAN-besturingsvliegtuiginfrastructuur
- Als u de bron-IP niet als legitiem kunt identificeren, kan dit wijzen op potentiële indicatoren van compromis
- Documenteer alle bevindingen en open onmiddellijk een TAC-zaak
- Neem de volledige opdrachtuitvoer op met peer-type en peer-systeem-ip-paren in uw geval
- 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 besturingscomponenten en open een TAC-geval om de bestanden te uploaden. TAC beoordeelt uw omgeving en geeft richtlijnen voor de volgende stappen.

V. Naar welke versie moet ik upgraden? A. Upgrade ten vroegste naar de dichtstbijzijnde vaste versie.

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 uw omgeving goed te beoordelen.

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 schakelt het PSIRT-team in en neemt contact met u op om de volgende stappen en richtlijnen voor uw omgeving te bespreken. Cisco voert de sanering niet namens u uit - TAC biedt de begeleiding die u nodig hebt om door te gaan.

V: Hoe weet ik welke vaste softwareversie ik moet gebruiken?

A: Raadpleeg de tabel Vaste softwareversies in dit document. TAC bevestigt de juiste versie voor uw specifieke omgeving.

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

A: Nee, wacht tot de TAC hun beoordeling heeft voltooid en advies heeft gegeven voordat u probeert herstelmaatregelen te nemen.

V: Wordt er downtime verwacht tijdens de sanering?

A: De impact hangt af van uw implementatiearchitectuur en het herstelpad. TAC biedt richtlijnen voor het minimaliseren van service-impact tijdens het proces.
V: Zijn de PSIRT-fixes opgenomen in de aankomende 20.15.5-release en andere aankomende releases?

A: Ja, fixes zijn opgenomen in 20.15.5 en andere aankomende releases. De upgrade om de in dit document beschreven kwetsbaarheden te verhelpen, moet echter ONMIDDELLIJK prioriteit krijgen. (Wacht niet!)

V: Moeten alle controllers worden bijgewerkt als er geen compromisindicatoren worden gevonden?

A: Ja, alle SD-WAN-besturingscomponenten (vManage, vSmart en vBond) moeten worden bijgewerkt naar een vaste softwareversie. Het upgraden van slechts een deel van de controllers is niet voldoende.

V: Ik heb een door de cloud gehoste SD-WAN-overlay. Wat zijn mijn opties voor een upgrade?

A: Voor cloud-gehoste 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 zelf met de upgradehandleidingen die in dit document beschikbaar zijn.
    - Open een stand-by TAC-case voor het onderhoudsvenster van uw voorkeur. TAC zal helpen als u problemen ondervindt met de upgrade.

V: Moeten we ook de edge-routers upgraden?

A: Cisco IOS XE-apparaten worden niet beïnvloed door dit advies.

V: Wij zijn een Cisco-gehoste overlay. Moeten we ACL's repareren of actie ondernemen op SSP?

A: Alle door Cisco gehoste klanten wordt geadviseerd om hun eigen toegestane inkomende regels te bekijken die op SSP te zien zijn en ervoor te zorgen dat alleen de noodzakelijke voorvoegsels van uw kant zijn toegestaan. Deze regels gelden alleen voor beheertoegang en zijn niet van toepassing op edge-routers. Bekijk ze in SSP > Overlay Details > Inkomende regels toestaan. Houd er rekening mee dat poort 22, 830 op dag 0 altijd standaard werden geblokkeerd door Cisco van buiten naar de cloud gehoste controllers.

V: We zijn op CDCS / Gedeelde huurder. Naar welke versie wordt er geüpgraded?

A: Op basis van de huidige versie zijn de gedeelde huurder of CDCS-clusters momenteel op schema om te worden bijgewerkt OF al te worden bijgewerkt naar de vaste versies. Hier zijn de gedeelde tenant en CDCS vaste releases:

1. Early Adopter clusters => 20.18.2.1 (dit is eigenlijk hetzelfde als de standaard release)

2. Releaseclusters aanbevelen => 20.15.405 (CDCS-specifieke versie met PSIRT-oplossingen)

CDCS-klanten hoeven geen actie te ondernemen om deze PSIRT effectief aan te pakken.

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

A: 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.