Remediate Catalyst SD-WAN Security Advisory - mei 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 14 mei 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-controllerverificatie omzeilt kwetsbaarheid
- Cisco Catalyst SD-WAN-kwetsbaarheden

Deze gebreken worden behandeld door deze PSIRT-adviezen:

- Cisco bug ID CSCwt50498
- Cisco bug ID CSCwt38739
- Cisco bug ID CSCwt38767
- Cisco bug ID CSCwt55544

Overzicht van de werkstroom voor probleemoplossing

Opmerking: Alle SD-WAN-controllers en -beheerders zijn kwetsbaar en vereisen een onmiddellijke upgrade voor alle besturingscomponenten. Niet alle controleurs tonen echter tekenen van compromis.

Vereiste actie: verzamel admin-techs, upgrade naar een vaste release en open vervolgens een Cisco TAC-case zodat TAC uw admin-techs kan scannen op indicatoren van compromis.

De TAC is beschikbaar voor:

- Scan de admin-techs die je aanbiedt voor indicatoren van compromis
- Upgradeondersteuning bieden als u problemen ondervindt tijdens de upgrade
- Begeleid u door aanvullende sanering als er compromisindicatoren worden geïdentificeerd

1. Verzamel Admin-Techs - Voer admin-tech uit op alle besturingscomponenten (vSmart, vManage, vBond) voorafgaand aan de upgrade om ervoor te zorgen dat er geen diagnostische gegevens verloren gaan. Selecteer Logboekopties en Technische opties. De kern is niet nodig.

   

Let op: vSmart-beheerderstechnieken mogen niet gelijktijdig worden uitgevoerd — voer ze één voor één uit. Alle andere kunnen in elke volgorde worden verzameld

2. Upgrade naar een vaste release - Upgrade alle SD-WAN-besturingscomponenten (vManage, vSmart, vBond) naar een vaste softwareversie die wordt vermeld in de tabel met vaste softwareversies.

Opmerking: wacht niet op de resultaten van de TAC-scan voordat u een upgrade uitvoert. Upgraden naar een vaste release heeft 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 logbundels met beheerderstechnologie die in stap 1 zijn verzameld. TAC scant de admin-techs voor indicatoren van compromis.
4. Als er een compromis is vastgesteld, volgt u de TAC-richtsnoeren - Als de TAC-indicatoren voor een compromis in uw omgeving vaststelt, vult u alle door de TAC verstrekte richtsnoeren voor herstel in. Als er geen compromisindicatoren worden gevonden, is geen verdere actie buiten de upgrade vereist.

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

Vereist: verzamel admin-tech bestanden van alle besturingscomponenten 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: 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: Upgrade naar een vaste softwareversie

Na het verzamelen van admin-techs in stap 1, upgrade alle SD-WAN-besturingscomponenten (vManage, vSmart en vBond) naar een vaste softwareversie.

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

Selecteer de juiste versie in de tabel Vaste softwareversies in dit document.

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

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

Stap 3: Open een TAC-zaak en upload Admin-Tech-bestanden

voor scannen

Na het upgraden in stap 2 opent u een ondersteuningscase voor Cisco TAC en uploadt u de in stap 1 verzamelde admin-tech-bestanden. TAC scant de admin-techs voor indicatoren van compromis.

Vereiste acties:

1. Open een TAC-geval voor prioriteitsniveau 3 met "CVE-2026-20182" en de relevante PSIRT-ID in de titel om het scanproces te starten.
2. Upload ALLE logboekbundels voor beheerderstechnologie die in stap 1 zijn verzameld (controllers, beheerders en validators)
3. Wacht tot TAC de scan heeft voltooid en de resultaten heeft meegedeeld

---

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

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

Als TAC compromisindicatoren in uw omgeving identificeert, neemt TAC contact met u op met specifieke richtlijnen voor herstel. Vul alle instructies in die door TAC worden verstrekt.

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

Vaste softwareversies

Deze softwarereleases bevatten oplossingen voor de geïdentificeerde kwetsbaarheden:

Geldt voor huidige versies	Vaste versie	Beschikbare software
20,3, 20,6, 20,9	20.9.9.1	20.9.9.1 Upgrade-images voor vManage, vSmart en vBond
20 .10, 20 .11, 20.12.5 en eerder in 30 .12	20.12.5.4	20.12.5.4 Upgrade-images voor vManage, vSmart en vBond
20 12 6 x	20.12.6.2	20.12.6.2 Upgrade-images voor vManage, vSmart en vBond
20.12.7	20.12.7.1	20.12.7.1 Upgrade-images voor vManage,

Geldt voor huidige versies	Vaste versie	Beschikbare software
		vSmart en vBond
20.13, 20.14, 20.15.4.3 en eerder in 20.15	20.15.4.4	20.15.4.4 Upgrade-images voor vManage, vSmart en vBond
20 15 5 x	20.15.5.2	20.15.5.2 Upgrade-images voor vManage, vSmart en vBond
20,16, 20,17, 20,18,x	20.18.2.2	20.18.2.2 Upgrade-images voor vManage, vSmart en vBond

Opmerking: Voor klanten op SD-WAN Cloud (voorheen bekend als Cloud Delivered Cisco Catalyst SD-WAN [CDCS]), de 20.15.506 is ook een vaste release. Dit is specifiek van toepassing op de door Cisco gehoste clusterimplementatie en wordt afzonderlijk van het standaard upgradepad behandeld. Al deze klanten zijn al geüpgraded naar de vaste release 20.15.506.

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 opdracht this uit om te zoeken in de glob van het vsyslog*-bestand:

```
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
```

Herhaal dit voor messages* file glob en vdebug* file glob.

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

Verificatie 3: Controleren op ontbrekende challenge-ack op Active Control-aansluitingen

Deze controle inspecteert de detailuitvoer van de besturingsverbindingen voor peer-sessies die worden gerapporteerd als actief (of onlangs afgebroken), maar de verwachte `challenge-ack`-uitwisseling missen. Een sessie die `hello`-pakketten in beide richtingen uitwisselt en `challenge-ack 0` toont in de Tx- of Rx-statistieken, geeft aan dat de peer nooit de verwachte challenge-handshake heeft voltooid - een anomalie die onderzoek rechtvaardigt. Voer dit uit op alle besturingscomponenten (controllers, beheerders en validators).

Stap 1: Verzamel de detailuitvoer van de besturingsverbindingen

Voer vanaf de CLI van het apparaat het volgende uit:

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

Sla de uitvoer op in een bestand (bijvoorbeeld `vdaemon.txt`) voor inspectie.

Stap 2: Waar moet je op letten

Markeer voor elke peer record (begrensd door `REMOTE-COLOR-` / `SYSTEM-IP-`headers) de record als al deze voorwaarden waar zijn:

- De sessiestatus is OMHOOG of TEAR_DOWN
- Zowel de Tx Statistics hello counter als de Rx Statistics hello counter zijn niet-nul (hellos stromen in beide richtingen)
- challenge-ack is 0 in het blok Tx-statistieken of Rx-statistieken (of beide)

Voorbeeld overeenkomende record (let op de `<<<<` pijlen die de ontbrekende `challenge-ack` markeren)

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

  Tx Statistics-
```

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

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

In het bovenstaande voorbeeld zijn zowel Tx- als Rx-`hello`-tellers niet-nul (actieve verbinding), maar `challenge-ack` is `0` in beide richtingen.

Stap 3: Handmatig zoeken, opdracht

Als u snel kandidaat-records wilt weergeven van een opgeslagen `vdaemon.txt` (of een bestand dat de `detailuitvoer voor controleverbindingen` bevat), voert u het volgende uit:

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

Elk teruggegeven blok vertegenwoordigt een peer-sessie waarbij `challenge-ack` wordt gerapporteerd als `0`. Controleer elk blok volledig om te bevestigen dat de `staat omhoog` is of `tear_down` en dat de `hello` tellers in zowel Tx als Rx niet-nul zijn voordat u het als een hit behandelt.

Stap 4: Resultaten en document voor TAC interpreteren

Als geen van de records aan alle drie de voorwaarden voldoet:

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

Als een of meer records aan alle drie de voorwaarden voldoen:

- Controleer zorgvuldig de waarden `SYSTEM-IP-`, `private-ip` en `public-ip` voor elk gemarkeerd record
- Controleer of de peer geen bekend, legitiem onderdeel is van uw SD-WAN-besturingsvlak (clusterlid, DR-site, IP-adres dat eerder aan een component is toegewezen)
- Als u de peer niet als legitiem kunt identificeren, kan dit wijzen op potentiële indicatoren van compromis
- Documenteer alle bevindingen en open onmiddellijk een TAC-zaak
- Voeg de volledige overeenkomende peer-record(s) en de uitvoer van de bronopdracht in uw geval toe

- 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 upgrade vervolgens alle besturingscomponenten 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. 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: Is er een manier waarop ik mijn eigen geautomatiseerde scan kan uitvoeren met behulp van TAC-tooling?

A: Klanten kunnen ook gebruik maken van de self-service "Check Bug Applicability" tool die is ingebouwd op de Bug Search Tool Page voor Cisco bug ID CSCwt50498 om admin-techs van de Control Components opnieuw te scannen.

V: Wat gebeurt er als er compromisindicatoren worden vastgesteld?

A: TAC neemt contact met u op om de volgende stappen en specifieke 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: Ja. Verzamel admin-techs, upgrade naar een vaste release en open vervolgens een TAC-case zodat TAC de admin-techs kan scannen op indicatoren van compromis.

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: 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 is beschikbaar om u te helpen als u problemen ondervindt met de upgrade.

V: Moeten we ook de edge-routers upgraden?

A: Nee, 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 SD-WAN Cloud (voorheen bekend als Cloud Delivered Cisco Catalyst SD-WAN [CDCS]). Naar welke versie wordt er geüpgraded?

A: Op basis van de huidige versie zijn SD-WAN Cloud-clusters momenteel op schema om te worden geüpgraded OF al te worden geüpgraded naar de vaste versies. Hier zijn de SD-WAN Cloud (voorheen CDCS) vaste releases:

1. Early Adopter clusters = 20.18.2.2 (dit is eigenlijk hetzelfde als de standaard release)

2. Releaseclusters aanbevelen = 20.15.506 (CDCS-specifieke versie met PSIRT-fixes)

SD-WAN Cloud-klanten hoeven geen actie te ondernemen om deze PSIRT effectief aan te pakken.

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

A: Op basis van de huidige versie zijn de gedeelde huurders momenteel op schema om te worden bijgewerkt OF al te worden bijgewerkt naar de vaste versies. Hier zijn de gedeelde vaste releases van de huurder:

1. Aanbevolen vrijgaveclusters = 20.15.5.2

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

A: Cisco TAC kan klanten helpen door te scannen op Indicators of Compromise (IoC's) die verband houden met deze kwetsbaarheden. TAC voert echter geen diepgaande forensische analyse of incidentonderzoek uit. Voor uitgebreid forensisch werk of gedetailleerde veiligheidsonderzoeken raden we klanten aan om hun favoriete externe Incident Response (IR)-bedrijf in te schakelen.

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.

V: We zien logboeken van een "root" -gebruiker op ons systeem. Is dit zorgwekkend?

A: Controleer wat er op dat moment nog meer in het systeem gebeurt. Deze logs zijn volledig te verwachten. Zo worden bijvoorbeeld logboeken voor systeemaanmelding-wijziging van een "root"-gebruiker weergegeven wanneer admin-techs worden gegenereerd. Logs kunnen ook worden gezien van een "root" -gebruiker tijdens een reboot.

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

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

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

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

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.