

Vet controleren op reeds bestaande artikelen

Inhoud

[Inleiding](#)

[Referenties — Cisco SD-WAN CVE-2026-20182 Documentatie](#)

[E-mails](#)

[Sherlock 1 - Intake - Upgrade aanvragen & Admin-Tech Files](#)

[Sherlock 2 - Resultaat - Geen IoC's geobserveerd \(per bestand\)](#)

[Sherlock 3 - Herinnering - Ontbrekende Admin-Tech-bestanden](#)

[TAC 1 - Onderzoek - Verdere evaluatie vereist \(IoC vermoed\)](#)

[TAC 2 - Resultaat - Geen IoC's gevonden \(door technicus bevestigd\)](#)

[TAC 3 - Validatie - Bevestig IP-eigendom in overlay](#)

[TAC 4 - Resultaat - vals positief gezuiverd](#)

[TAC 5 - Kritiek - Identificatie van het IoC, oproep tot herziening planning](#)

[TAC 6 - Resultaat - IvO dupliceren \(Close & Redirect\)](#)

[TAC 7 - Herstel - Opties voor follow-up \(na oproep\)](#)

[TAC 8 - Remediation - Bijgewerkte opties voor gecompromitteerde stoffen \(Optie 2 follow-up\)](#)

[TAC 17 - Omgekeerde bevinding - Voorheen geen IoC, nu IoC geïdentificeerd \(CVE-2026-20182\)](#)

[CloudOps 1 - Proactief - IoC gedetecteerd in Cloud Scan, Admin-Tech vereist om te valideren](#)

[E-mails voor WAVE 2A voor klanten met een eerdere impact die de opties A, B of C nog niet hebben voltooid. \(Opties 1 en 2 moeten opnieuw worden uitgevoerd\)](#)

[TAC 9 Template for no IOC for PSIRT2a/they did rebuild \(voorheen beïnvloed\)](#)

[TAC 10-sjabloon voor ja IOC voor PSIRT2a / ze hebben herbouwd \(eerder beïnvloed\)](#)

[TAC 11 Template for no IOC for PSIRT2a/they did not rebuild \(previously IMPACTED\)](#)

[TAC 12 Template for yes IOC for PSIRT2a/they did not rebuild \(previously IMPACTED\)](#)

[E-mails voor WAVE 2A voor nieuwe klanten \(niet eerder beïnvloed\)](#)

[TAC 13 Template for no IOC / No Fixed Release Available \(WAVE 2a — Await Fix\)](#)

[TAC 14 Template for no IOC / Fixed Release Available \(WAVE 2a — Upgrade Now\)](#)

[TAC 15-sjabloon voor IOC-geïdentificeerde / vaste release beschikbaar \(WAVE 2a - dringende upgrade\)](#)

[TAC 16 Template for IOC Identified / No Fixed Release Available \(WAVE 2a — Harden & Await Fix\)](#)

Inleiding

In dit document worden de goedgekeurde e-mailsjablonen van klanten gecentraliseerd die worden gebruikt tijdens het triëren en oplossen van problemen die verband houden met de Cisco Catalyst SD-WAN Controller Authentication Bypass-kwetsbaarheid. Sjablonen worden gesplitst op afzender - Sherlock (geautomatiseerde case-uitwisselingen die admin-tech-gegevens verzamelen en voorlopige IoC-resultaten retourneren) en TAC-ingenieur (door mensen aangestuurde follow-

ups voor onderzoek, validatie en remediëringsrichtlijnen).

Referenties — Cisco SD-WAN CVE-2026-20182 Documentatie

Hoofddijst van elk Cisco-document waarnaar in de bovenstaande e-mailsjablonen wordt verwezen. Nummering is uniform — superscripts per e-mail (bijv. ^[2]) verwijzen naar de items in deze lijst.

1. **Cisco SD-WAN Hardening Guide** — <https://sec.cloudapps.cisco.com/security/center/resources/Cisco-Catalyst-SD-WAN-HardeningGuide>
2. **Officieel veiligheidsadvies (cisco-sa-sdwan-mltnps2-JxpWm7R)** — <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-mltnps2-JxpWm7R>
3. **Handleiding voor TAC-herstel** — <https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/225842-remediate-catalyst-sd-wan-security.html#toc-hld--1516256622>
4. **Cisco SD-WAN Upgrade Guide** — <https://www.cisco.com/c/en/us/support/docs/wan/dpt/220424-upgrade-sd-wan-controllers-with-the-use.html>
5. **Cisco SD-WAN Admin-Tech Collection Guide** — <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. **Tweede beveiligingsadvies (cisco-sa-sdwan-rpa2-v69WY2SW)** — <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa2-v69WY2SW>
7. **Uw Catalyst SD-WAN-upgrade starten** — <https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/225515-start-your-catalyst-sd-wan-upgrade.html>

E-mails

Sherlock 1 - Intake - Upgrade aanvragen & Admin-Tech Files

Use case

Eerste bereik wanneer een TAC-zaak wordt geopend voor CVE-2026-20182 om te adviseren admin-tech-gegevens te verzamelen van en vervolgens alle SD-WAN-besturingscomponenten te upgraden.

onderwerp

Belangrijk: actie vereist voor CVE-2026-20182 - Upgradeplanning en loC-beoordeling

bericht

Geachte klant,

Bedankt voor het contact opnemen met het Cisco Technical Assistance Center (TAC).

Wat betreft de kwetsbaarheid in verband met **CVE-2026-20182**, raadpleeg het [officiële veiligheidsadvies](#)^[1] voor volledige details en de [TAC-remediëringsgids](#)^[2].

Ons primaire doel is om uw omgeving te helpen beveiligen. Geef **prioriteit aan uw upgradeplanning en -uitvoering** als de meest kritieke stap om dit risico te beperken. Als u deze upgrade nog niet hebt gepland, moet u dit onmiddellijk doen.

Upgradebronnen: raadpleeg het volgende officiële Cisco-document voor gedetailleerde instructies over het uitvoeren van de upgrade: [Cisco SD-WAN Upgradehandleiding](#)^[3]

Om een eerste beoordeling van uw omgeving mogelijk te maken voor potentiële indicatoren van compromis (IoC's) met betrekking tot CVE-2026-20182, moet u een admin-tech-verzameling uitvoeren *voorafgaand* aan de upgrade. Volg deze volgorde van bewerkingen:

1. **Verzamel Admin-Tech-bestanden:** Genereer de logboeken van alle SD-WAN-besturingscomponenten voorafgaand aan de upgrade om ervoor te zorgen dat er geen diagnostische gegevens verloren gaan. Zorg ervoor dat u zowel "Logs" als "Tech" selecteert bij het genereren van deze bestanden.
 - **vSmarts (Controllers):** Verzamel één tegelijk, niet tegelijkertijd.
 - **vBonds (Validators):** Verzamelen van alle knooppunten.
 - **Beheer (vManage):** Verzamelen van alle knooppunten in het cluster (actieve en stand-by DR).
2. **Upgrade uitvoeren:** Upgrade alle SD-WAN-besturingscomponenten (vManage, vSmart, vBond) naar een vaste softwareversie die in het advies wordt vermeld. Wacht niet op de analyse van het admin-tech-logboek voordat u begint met upgraden, omdat de upgrade het beveiligingslek onmiddellijk sluit.
3. **Uploaden naar TAC Case:** Zodra de upgrade is voltooid, uploadt u de eerder verzamelde bestanden naar uw bestaande TAC-case tegelijkertijd, indien mogelijk. Ons team zal vervolgens een scan van deze logs uitvoeren om uw omgeving te beoordelen op Indicators of Compromise (IoC's).

Middelen en ondersteuning:

Voor meer details en stapsgewijze instructies over het genereren en veilig indienen van uw admin-tech-bestanden, raadpleegt u deze handleiding: [Cisco SD-WAN Admin-Tech Collection Guide](#)^[4].

Als u een BCS/LCS-abonnement hebt, neemt u contact op met uw Cisco NCE of Delivery Manager voor meer informatie

over het upgradeproces of de volgende stappen.

Uw privacy en veiligheid blijven onze topprioriteit. Alle verstrekte informatie wordt behandeld in overeenstemming met het privacy- en beveiligingsbeleid van Cisco.

U ontvangt een automatische bevestiging per e-mail voor **ELK** bestand dat met succes naar de kwestie is geüpload. Controleer deze meldingen.

Bedankt voor de snelle samenwerking bij het beveiligen van uw infrastructuur.

Links:

- [1] [Officiële veiligheidsadviseur](#)
- [2] [Handleiding voor TAC-herstel](#)
- [3] [Upgradehandleiding voor Cisco SD-WAN](#)
- [4] [Cisco SD-WAN Admin-Tech Collectiehandleiding](#)

Met vriendelijke groeten,

Openen in Outlook

Gebruik de .eml download hieronder. Vervang alle **[tussen haakjes geplaatste plaatsaanduidingen]** vóór verzending.

✉ Open Outlook (alleen onderwerp)

⬇ Download .eml Template

Sherlock 2 - Resultaat - Geen IoC's geobserveerd (per bestand)

Use case

Verzonden na admin-tech analyse toont geen waargenomen indicatoren van compromis voor een specifiek geüpload bestand. Wordt eenmaal per verwerkt bestand verzonden.

onderwerp

Update: Analyseresultaten voor SD-WAN-component [Bestandsnaam invoegen] – CVE-2026-20182

bericht

Geachte klant,

Dank u voor uw geduld.

We hebben de analyse van het admin-tech bestand [Bestandsnaam invoegen] voltooid. In dat bestand hebben we geen

indicatoren van compromis met betrekking tot CVE-2026-20182 voor dit specifieke apparaat geïdentificeerd.

Houd er rekening mee dat de hoeveelheid logboekgegevens die u hebt opgehaald en aan Cisco hebt verstrekt voor deze beoordeling mogelijk is beperkt door de logboekbewaarperiode die u hebt geconfigureerd volgens de **Cisco SD-WAN Hardening Guide**^[1].

Belangrijk: volgende stappen en sluiting van de zaak:

1. **Wacht op alle resultaten:** houd er rekening mee dat de resultaten in deze e-mail een gedeeltelijk resultaat kunnen zijn. We zullen elk bestand analyseren zoals het is verstrekt. Wacht totdat u een bevestiging hebt ontvangen voor alle geüploade bestanden voordat u de beoordeling als voltooid beschouwt.
2. **Upgradeprioriteit:** Hoewel de voorlopige scans van admin-tech-logs geen compromisindicatoren (IoC's) hebben geïdentificeerd, kan de onderliggende kwetsbaarheid blijven bestaan. Voor Cisco Cloud-Pro- en Cisco On-Prem- implementaties, als u dit nog niet hebt gedaan, geeft u prioriteit aan de volledige upgrade van uw SD-WAN- besturingscomponenten zo snel mogelijk.
 - Cisco Cloud (fka: SaaS) klantstructuren worden automatisch bijgewerkt door Cisco als onderdeel van de beheerde service. Geen actie nodig.
3. **Case Closure:** Zodra u "no observed IoC" -resultaten hebt ontvangen voor al uw geüploade bestanden EN (indien van toepassing) u de software-upgrade in uw omgeving met succes hebt voltooid, kunt u deze zaak als opgelost beschouwen en doorgaan met standaard afsluitingsprocedures.

Upgrade Resources (indien van toepassing): Raadpleeg het volgende officiële Cisco-document voor gedetailleerde instructies over het uitvoeren van de upgrade voor Cisco Cloud-Pro en Cisco On-Prem: Cisco SD-WAN Upgrade Guide

Een overzicht op hoog niveau van het upgradeproces omvat:

1. De juiste software-images uploaden naar uw Manager (vManage)-opslagplaats.
2. Volgend op uw controllers upgraden, te beginnen met Manager (vManage), gevolgd door Validator (vBond) en Controller (vSmart).
3. De nieuwe softwareversies activeren en de systeemfunctionaliteit valideren.

Wij zullen uw zaak blijven volgen. Als we niet binnen 10 werkdagen nadat we alle resultaten hebben verstrekt op basis van bestanden die we van u hebben ontvangen, terug horen, gaan we ervan uit dat er geen verdere hulp nodig is en gaan we verder met de normale TAC-procedures voor de sluiting van de zaak. Mocht u op enig moment hulp nodig hebben, laat het ons dan weten.

Met vriendelijke groeten,

Openen in Outlook

Vervang alle [tussen haakjes geplaatste plaatsaanduidingen] vóór verzending.

✉ Open Outlook (alleen onderwerp)

⬇ Download .eml Template

Sherlock 3 - Herinnering - Ontbrekende Admin-Tech-bestanden

Use case

Geautomatiseerde follow-up wanneer de ingediende admin-tech bestanden niet overeenkomen met het aantal SD-WAN controle componenten gevonden in logs.

onderwerp

Herinnering: ontbrekende Admin-Tech-bestanden vereist voor CVE-2026-20182-beoordeling

bericht

Geachte klant,

We missen nog steeds admin-techs van uw SD-WAN-besturingscomponenten, dus ons systeem kan geen compromisindicatoren beoordelen uit de logboeken van de admin-tech. Om de CVE-2026-20182-beoordeling te starten, moeten we beheerderstechnologiebestanden ontvangen van ALLE controllers (vSmarts), validators (vBonds) en managers (vManage), inclusief alle Manager (vManage) -knooppunten indien geclusterd.

Volgende stappen:

Upload de resterende admin-tech bestanden op uw vroegst gemak.

Met vriendelijke groeten,

Openen in Outlook

Vervang alle **[tussen haakjes geplaatste plaatsaanduidingen]** vóór verzending.

✉ Open Outlook (met body)

⬇ Download .eml Template

TAC 1 - Onderzoek - Verdere evaluatie vereist (IoC vermoed)

Use case

Verzonden door TAC-ingenieur zodra automatisering logboeken heeft gevonden die mogelijke compromissen aangeven en menselijk onderzoek vereist is.

onderwerp

SR # - nader onderzoek nodig

bericht

Geachte klant,

Mijn naam is {your_name} en ik heb uw zaak aanvaard. Hartelijk dank voor de samenwerking met het Cisco Technical Assistance Centre (TAC).

Na een voorlopige analyse van de admin-tech-bestanden die u hebt verstrekt van uw **SD-WAN-besturingscomponenten**, hebben we vastgesteld dat verder TAC-onderzoek nodig is om onze analyse te voltooien. Om te zorgen voor een grondige en nauwkeurige oplossing, zal ik nauw met u samenwerken aan de volgende stappen.

U kunt er zeker van zijn dat we vastbesloten zijn om u te ondersteunen tijdens deze volgende stappen en duidelijke richtlijnen zullen geven om de situatie effectief aan te pakken.

Geef prioriteit aan de planning en uitvoering van uw upgrade als de meest kritieke stap om dit risico te beperken. Als u deze upgrade nog niet hebt gepland, moet u dit onmiddellijk doen.

Als u vragen heeft of hulp nodig heeft, aarzel dan niet om contact op te nemen met uw TAC-ingenieur.

Bedankt voor uw aandacht en medewerking.

Met vriendelijke groeten,

Openen in Outlook

Vervang alle [tussen haakjes geplaatste plaatsaanduidingen] vóór verzending.

✉ Open Outlook (met body)

⬇ Download .eml Template

TAC 2 - Resultaat - Geen IoC's gevonden (door technicus bevestigd)

Use case

Verzonden door TAC-ingenieur zodra de automatisering geen compromisindicatoren heeft gevonden en de ingenieur het resultaat heeft bevestigd.

onderwerp

bericht

Hallo [klantnaam],

Ik ben de Cisco TAC-ingenieur toegewezen aan uw zaak [SR-nummer].

Na het uitvoeren van een voorlopige scan van de admin-tech-bestanden die u hebt verstrekt van uw SD-WAN-besturingscomponenten, hebben we geen logboekvermeldingen gevonden die consistent zijn met compromisindicatoren die worden beschreven in de Cisco SD-WAN Security Advisories:

- **Cisco Catalyst SD-WAN Controller Authentication Bypass Vulnerability [1]**
- **Cisco Catalyst SD-WAN Manager-kwetsbaarheden [2]**

U moet echter doorgaan met het upgraden van al uw SD-WAN-besturingscomponenten naar <versie invoegen>. Hier zijn de stappen om verder te gaan met de upgrade:

- **Start uw Catalyst SD-WAN-upgrade [3]**
- **Cisco SD-WAN-upgradehandleiding[4]**

Houd er rekening mee dat Cisco niet in staat is om logs van edge-apparaten te beoordelen vanwege de dynamische aard van IP-adressering op internet en ons gebrek aan kennis van verwachte IP-adressen van edge-apparaten in het netwerk van een klant. Klanten worden aangemoedigd om de Peering Event Validation Guidance te volgen die wordt vermeld in de Cisco Catalyst SD-WAN Controller Authentication Bypass Vulnerability Security Advisory om deze stap handmatig uit te voeren. Klanten worden ook aangemoedigd om de aanvullende detectiestappen met betrekking tot de validatie van peering-gebeurtenissen uit te voeren, zoals beschreven in de beveiligingsadvies voor CVE-2026-20182.

links

[1] Cisco Catalyst SD-WAN Controller Authentication Bypass Vulnerability -

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

[2] Cisco Catalyst SD-WAN Manager-kwetsbaarheden -

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

[3] Start uw Catalyst SD-WAN-upgrade — <https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/225515-start-your-catalyst-sd-wan-upgrade.html>

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

Met vriendelijke groet,

Openen in Outlook

Vervang alle *[tussen haakjes geplaatste plaatsaanduidingen]* vóór verzending.

✉ Open Outlook (alleen onderwerp)

↓ Download .eml Template

TAC 3 - Validatie - Bevestig IP-eigendom in overlay

Use case

Verzonden door TAC-technicus om de klant te vragen of specifieke IP-adressen die zijn opgedoken tijdens loganalyse deel uitmaken van hun SD-WAN-overlay-infrastructuur.

onderwerp

[SR #] – Validering van IP-adres vereist

bericht

Geachte [Naam van klant],

Mijn naam is [Your Name] en ik ben de Cisco TAC-ingenieur die aan uw zaak is toegewezen.

Als onderdeel van onze doorlopende analyse van de admin-tech-bestanden die u hebt verstrekt vanuit uw SD-WAN-besturingscomponenten, hebben we uw hulp nodig bij het valideren of de volgende IP-adressen deel uitmaken of eerder deel uitmaakten van uw SD-WAN-overlay-infrastructuur:

IP-adres(sen):

- [IP-adres 1]

- [IP-adres 2]

Om ons te helpen onze beoordeling te voltooien, bevestigt u:

1. Is dit IP-adres momenteel gekoppeld aan een component in uw SD-WAN-overlay (bijv. vManage, vSmart, vBond of edge-apparaat)?
2. Werd dit IP-adres eerder gebruikt door een SD-WAN-besturingscomponent die mogelijk buiten bedrijf is gesteld of waarvan het IP is gewijzigd?
3. Is dit IP-adres gekoppeld aan een Disaster Recovery (DR)-site of een andere infrastructuur met betrekking tot uw SD-WAN-implementatie?

Uw snelle reactie stelt ons in staat om onze analyse voort te zetten en u de juiste volgende stappen te bieden.

Als u vragen heeft, aarzel dan niet om contact op te nemen.

Met vriendelijke groeten,

Openen in Outlook

Alle [tussen haakjes geplaatste plaatsaanduidingen] vervangen voordat u ze verzendt.

✉ Open Outlook (met body)

↓ Download .eml Template

TAC 4 - Resultaat - vals positief gezuiverd

Use case

Verzonden door TAC-ingenieur na een handmatige beoordeling bepaalt dat de initiële loC gemarkeerd door geautomatiseerd scannen een vals positief was.

onderwerp

Update: Technische beoordeling voor CVE-2026-20182 – Case [Case Number]

bericht

Geachte klant,

Bedankt voor uw geduld terwijl ons engineeringteam een handmatige beoordeling uitvoerde van de admin-tech-bestanden die u hebt verstrekt vanuit uw SD-WAN-besturingscomponenten.

Na een grondig onderzoek hebben we vastgesteld dat de initiële indicator van het compromis (loC) die door ons geautomatiseerde scanproces is gemarkeerd, een vals positief was, d.w.z. dat onze beoordeling is dat de loC's niet geldig zijn.

Belangrijk: hoewel deze specifieke waarschuwing is gewist, moet u er rekening mee houden dat de kwetsbaarheid in verband met [CVE-2026-20182](#)^[1] een software-upgrade vereist om de veiligheid en integriteit van uw SD-WAN-verbinding op de lange termijn te garanderen.

Als u de upgrade nog niet hebt voltooid: Geef prioriteit aan de volledige upgrade van uw SD-WAN-besturingscomponenten zo snel mogelijk. De upgrade is de enige manier om deze kwetsbaarheid effectief te verhelpen. Raadpleeg de [Cisco SD-WAN Upgrade Guide](#)^[2] voor gedetailleerde instructies.

Als u de upgrade al hebt voltooid: aangezien we deze bevinding als vals positief hebben bevestigd en u de softwareremediatie al hebt uitgevoerd, is geen verdere actie vereist. U kunt deze zaak als opgelost beschouwen en doorgaan met de standaardprocedures voor afsluiting.

Wij waarderen uw inzet bij het prioriteren van de beveiliging van uw infrastructuur. Mocht u nog vragen hebben of extra hulp nodig hebben, aarzel dan niet om contact met ons op te nemen.

Met vriendelijke groeten,
Cisco Technical Assistance Centre (TAC)

Links:

[1] [Officiële veiligheidsadviseur](#)

[2] [Upgradehandleiding voor Cisco SD-WAN](#)

Openen in Outlook

Vervang alle *[tussen haakjes geplaatste plaatsaanduidingen]* vóór verzending.

✉ Open Outlook (alleen onderwerp)

⬇ Download .eml Template

TAC 5 - Kritiek - Identificatie van het IoC, oproep tot herziening planning

Use case

Verzonden door TAC-technicus wanneer potentiële compromisindicatoren zijn bevestigd en een dringend telefoontje van de klant vereist is om bevindingen en volgende stappen te bespreken.

onderwerp

URGENT: Analyseresultaten voor CVE-2026-20182 – Indicator van compromis geïdentificeerd

bericht

Geachte klant,

Dank u voor uw geduld terwijl we de admin-tech-bestanden analyseerden die voor uw SD-WAN-besturingscomponenten werden geleverd.

Naar aanleiding van onze technische evaluatie hebben we potentiële indicatoren van compromissen (IoC's) vastgesteld met betrekking tot CVE-2026-20182.

Gezien de aard van deze bevindingen is het van cruciaal belang dat we de technische details en de aanbevolen volgende stappen zo snel mogelijk bespreken. We willen graag een gesprek met uw team plannen om de specifieke bevindingen te bekijken en de juiste remediëring te bespreken.

Volgende stappen:

- **Een vergadering plannen:** laat ons weten dat u binnen de volgende [bijv. 4-8 uur] beschikbaar bent voor een kort gesprek om deze bevindingen te bekijken.
- **Upgrade SDWAN-besturingscomponenten:** upgrade uw SDWAN-beheer, -controller en -validator zo snel mogelijk naar een vaste release.

Ons primaire doel is om u te helpen bij het beveiligen van uw omgeving en het beperken van mogelijke risico's. Wij waarderen uw snelle aandacht voor deze zaak en kijken ernaar uit om met u te coördineren.

Met vriendelijke groeten,

Openen in Outlook

Vervang alle [tussen haakjes geplaatste plaatsaanduidingen] vóór verzending.

✉ Open Outlook (met body)

↓ Download .eml Template

TAC 6 - Resultaat - IvO dupliceren (Close & Redirect)

Use case

Verzonden door TAC-ingenieur wanneer IoC-analyse bevindingen bevestigt die overeenkomen met een eerdere SR voor dezelfde klant / omgeving. De huidige zaak is gesloten en de klant wordt doorverwezen naar de oorspronkelijke SR waar al een hersteladvies is verstrekt.

onderwerp

Update: Technische beoordeling voor CVE-2026-20182 – Case [SR #] (Duplicate IoC bevestigd)

bericht

Geachte klant,

Dank u voor uw geduld terwijl we de admin-tech-bestanden analyseerden die voor uw SD-WAN-besturingscomponenten werden geleverd. We hebben vastgesteld dat de initiële indicator(en) van het compromis (IoC) die door ons scanproces zijn gemarkeerd, dezelfde zijn als die welke al zijn gecommuniceerd in **[Original SR #]**. Zoals eerder besproken, raden we een dringende upgrade aan en gaan we verder met een van de twee herstelpaden die zijn beschreven in de [TAC-remediëringsgids](#)^[2] om uw omgeving zo snel mogelijk te beveiligen. Raadpleeg het [officiële veiligheidsadvies voor CVE-2026-20182](#)^[1] voor alle details.

Ik ga nu over tot sluiting van deze zaak. Gebruik **[Origineel SR-nummer]** om meer begeleiding of technische ondersteuning aan te vragen met betrekking tot uw upgrade of probleemoplossing.

Met vriendelijke groeten,
[Uw naam]

Links:

[1] [Officiële veiligheidsadviseur](#)

[2] [Handleiding voor TAC-herstel](#)

Openen in Outlook

Vervang alle *[tussen haakjes geplaatste plaatsaanduidingen]* vóór verzending.

✉ Open Outlook (met body)

⬇ Download .eml Template

TAC 7 - Herstel - Opties voor follow-up (na oproep)

Use case

Verzonden na de IoC-reviewoproep om de besproken herstelpaden samen te vatten. De klant kiest voor optie A (herimplementatie met doorlopende herstart), optie B (herimplementatie met harde cutover) of optie C (volledige systeemherbouw).

onderwerp

Follow-up: herstelopties voor CVE-2026-20182

bericht

Geachte klant,

Bedankt voor de tijd die je hebt genomen om de bevindingen van onze recente analyse te bespreken. Zoals we tijdens het vorige gesprek hebben besproken, raden we aan om door te gaan met een van de volgende herstelpaden om uw omgeving te beveiligen.

Optie A: Herplaatsing met doorlopende herstart. Prioriteert operationele continuïteit door netwerkdowntime te vermijden, hoewel dit een resterend risico op dreigingspersistentie tijdens het overgangsproces met zich meebrengt.

Omschrijving: Omvat herimplementatie van de controller, plus SSH-sleutel en certificaatrotatie. Bestaande controlleronderdelen worden tijdens de migratie via vManage verbonden om de nieuwe fabric te implementeren. Vervolgens worden ze verwijderd zodra het apparaat is gemigreerd.

Optie B: Herplaatsing met harde omslag. Biedt een hoger niveau van beveiliging. Omdat nieuwe controllers nooit verbinding maken met oude controllers, is er volledige isolatie. Dit heeft gevolgen voor de algemene netwerkactiviteiten, aangezien alle apparaten opnieuw verbinding moeten maken en route-/connectiviteitsinformatie moeten uitwisselen. Het tijdstip van uitval hangt af van het aantal sites, het aantal uitgewisselde voorvoegsels, enz.

Omschrijving: Omvat herimplementatie van de controller plus SSH-sleutel en rotatie van het certificaat, maar de oude controlleronderdelen worden tijdens herimplementatie van de nieuwe structuur geïsoleerd.

Optie C: Volledige systeemreconstructie. Biedt het hoogste niveau van beveiliging door een schone basislijn vast te stellen, hoewel dit de meest complexe aanpak is en een hoger risico op configuratiegerelateerde instabiliteit tijdens de wederopbouw met zich meebrengt. Dit is een langdurige optie en vereist expertise in het opnieuw opbouwen van het sjabloon en de beleidsdatabases.

Volgende stappen:

- Bespreek deze opties intern en laat ons weten welke weg u wilt inslaan. Zodra u een beslissing hebt genomen, kunnen we u verder begeleiden of technische ondersteuning bieden om u door de uitvoeringsfase te helpen.

Wij zijn er om u te ondersteunen tijdens dit proces. Laat het ons weten als u vragen heeft over deze opties.

Met vriendelijke groeten,

Cisco Technical Assistance Centre (TAC)

Optie 1 is de upgrade. Het scenario dat deze upgrade heeft uitgevoerd, is al uitgevoerd.

Openen in Outlook

Gebruik de .eml download hieronder. Vervang alle [tussen haakjes geplaatste plaatsaanduidingen] vóór verzending.

 Open Outlook (alleen onderwerp)

 Download .eml Template

TAC 8 - Remediation - Bijgewerkte opties voor gecompromitteerde stoffen (Optie 2 follow-up)

Use case

Klanten op de hoogte brengen van wie de SD-WAN-verbindingen zijn aangetast en eerder optie 2 hebben gevolgd en van wie wordt aangenomen dat de verbindingen het risico lopen dat de bedreigingsfactor blijft bestaan. Klanten die hun gecompromitteerde fabric opnieuw hebben gebouwd (en niet vertrouwd op een back-up/bestaande configuratiedatabase) worden niet geacht risico te lopen en zullen deze communicatie niet ontvangen. Deze mededeling zal door TBD worden verzonden.

onderwerp

bericht

Geachte klant,

We bieden een kritische update voor de sanering van uw SD-WAN-verbinding, zoals vermeld in [SR #] en de eerder gecommuniceerde beveiligingsadviezen. Deze update is specifiek voor stoffen waarin de verstrekte logboeken bewijs van compromisindicatoren (IOC's) vertoonden.

Hoewel u eerder een herstelplan hebt geselecteerd op basis van optie 2 — met een software-upgrade, herimplementatie van de controller en draaiing van SSH-sleutels — is onze analyse van het bedreigingslandschap blijven evolueren. Nieuwe technische inzichten met betrekking tot de exploitatie van deze kwetsbaarheden geven aan dat extra maatregelen dringend nodig zijn om het risico op persistentie te verminderen en de integriteit van de certificatenketen van vertrouwen te helpen waarborgen.

VEREISTE ACTIE:

We hebben de aanbevolen herstelstrategieën bijgewerkt om een uitgebreidere verdediging te bieden door aanvullende rotatie van rootcertificaten op te nemen.

Houd er rekening mee dat de herstelmaatregelen extra onderhoudsactiviteiten vereisen, waaronder geplande downtime van het netwerk.

Aangezien de veiligheid en integriteit van uw netwerk onze prioriteit is, hebben we drie verschillende herstelopties ontwikkeld. Elke optie hieronder biedt een balans tussen operationele impact en beveiligingsgarantie voor uw overweging. Omdat uw interne risicohouding uniek is, kan Cisco geen bepaald pad aanbevelen.

Optie A: Herplaatsing met doorlopende herstart. Prioriteert operationele continuïteit door netwerkdowntime te vermijden, hoewel dit een resterend risico op dreigingspersistentie tijdens het overgangsproces met zich meebrengt.

Omschrijving: Omvat herimplementatie van de controller, plus SSH-sleutel en certificaatroteratie. Bestaande controlleronderdelen worden tijdens de migratie via vManage verbonden om de nieuwe fabric te implementeren. Vervolgens worden ze verwijderd zodra het apparaat is gemigreerd.

Optie B: Herplaatsing met harde omslag. Biedt een hoger niveau van beveiliging. Omdat nieuwe controllers nooit verbinding maken met oude controllers, is er volledige isolatie. Dit heeft gevolgen voor de algemene netwerkactiviteiten, aangezien alle apparaten opnieuw verbinding moeten maken en route-/connectiviteitsinformatie moeten uitwisselen. Het tijdstip van uitval hangt af van het aantal sites, het aantal uitgewisselde voorvoegsels, enz.

Omschrijving: Omvat herimplementatie van de controller plus SSH-sleutel en rotatie van het certificaat, maar de oude controlleronderdelen worden tijdens herimplementatie van de nieuwe structuur geïsoleerd.

Optie C: Volledige systeemreconstructie. Biedt het hoogste niveau van beveiliging door een schone basislijn vast te

stellen, hoewel dit de meest complexe aanpak is en een hoger risico op configuratiegerelateerde instabiliteit tijdens de wederopbouw met zich meebrengt. Dit is een langdurige optie en vereist expertise in het opnieuw opbouwen van het sjabloon en de beleidsdatabases.

Zodra uw team deze opties heeft beoordeeld en de aanpak heeft geïdentificeerd die het beste aansluit bij uw risicomanagementnormen, laat het ons weten door op dit bericht te reageren. Na ontvangst van uw selectie, zullen wij het onderhoudsvenster coördineren en beginnen met de nodige technische voorbereidingen voor de uitvoering.

Wij stellen het op prijs dat u zich blijft richten op het onderhouden van een veilige netwerkinfrastructuur. Laat het ons weten als u verdere technische verduidelijking nodig hebt door een serviceverzoek (SR) te openen bij ons Technical Assistance Centre (TAC).

Met vriendelijke groet,
Cisco

Openen in Outlook

Gebruik de .eml download hieronder. Vervang alle **[tussen haakjes geplaatste plaatsaanduidingen]** vóór verzending.

✉ Open Outlook (alleen onderwerp)

⬇ Download .eml Template

TAC 17 - Omgekeerde bevinding - Voorheen geen loC, nu loC geïdentificeerd (CVE-2026-20182)

Use case

Verzonden naar klanten die eerder werden **geïnformeerd dat er geen indicatoren van compromis (loC's)** werden gevonden, maar voor wie een **daaropvolgende interne beoordeling** van logboeken van admin-technologie sindsdien **loC's** met betrekking tot CVE-2026-20182 heeft **geïdentificeerd**. Communiceert de herziene bevinding en biedt de drie herstelopties (optie A, B of C).

onderwerp

Belangrijke update: Herziene loC-beoordeling voor CVE-2026-20182 - Indicatoren van compromis nu geïdentificeerd - SR [SR#]

bericht

Geachte klant,

Bedankt voor uw voortdurende samenwerking met het Cisco Technical Assistance Center (TAC) met betrekking tot CVE-2026-20182 onder Serviceverzoek [SR#].

In onze vorige correspondentie hebben we geadviseerd dat onze analyse van de admin-tech-bestanden die worden geleverd vanuit uw SD-WAN-besturingscomponenten geen compromisindicatoren (IoC's) met betrekking tot dit advies identificeerde. Als onderdeel van onze voortdurende inzet voor uw beveiliging, hebben we sindsdien een routinematige interne beoordeling uitgevoerd van extra admin-tech loggegevens die zijn gekoppeld aan de structuur van uw organisatie.

Bij deze latere evaluatie zijn compromisindicatoren (IoC's) vastgesteld die tijdens de eerste beoordeling niet aan het licht zijn gekomen. We werken nu met u samen om deze bevindingen aan te pakken. Deze IoC's wijzen op mogelijk verdachte activiteiten binnen de structuur van uw organisatie die herstelacties rechtvaardigen.

We erkennen dat dit het eerder aan u gecommuniceerde resultaat herzielt en we willen ervoor zorgen dat u een duidelijk en nauwkeurig beeld heeft van uw omgeving, zodat de juiste sanering kan worden uitgevoerd.

VEREISTE ACTIE:

Houd er rekening mee dat de herstelmaatregelen extra onderhoudsactiviteiten vereisen, waaronder geplande downtime van het netwerk.

Aangezien de veiligheid en integriteit van uw netwerk onze prioriteit is, hebben we drie verschillende herstelopties ontwikkeld. Elke optie hieronder biedt een balans tussen operationele impact en beveiligingsgarantie voor uw overweging. Omdat uw interne risicohouding uniek is, kan Cisco geen bepaald pad aanbevelen.

Optie A: Herplaatsing met doorlopende herstart. Prioriteert operationele continuïteit door netwerkdowntime te vermijden, hoewel dit een resterend risico op dreigingspersistentie tijdens het overgangsproces met zich meebrengt.

Omschrijving: Omvat herimplementatie van de controller, plus SSH-sleutel en certificaatrotatie. Bestaande controlleronderdelen worden tijdens de migratie via vManage verbonden om de nieuwe fabric te implementeren. Vervolgens worden ze verwijderd zodra het apparaat is gemigreerd.

Optie B: Herplaatsing met harde omslag. Biedt een hoger niveau van beveiliging. Omdat nieuwe controllers nooit verbinding maken met oude controllers, is er volledige isolatie. Dit heeft gevolgen voor de algemene netwerkactiviteiten, aangezien alle apparaten opnieuw verbinding moeten maken en route-/connectiviteitsinformatie moeten uitwisselen. Het tijdstip van uitval hangt af van het aantal sites, het aantal uitgewisselde voorvoegsels, enz.

Omschrijving: Omvat herimplementatie van de controller plus SSH-sleutel en rotatie van het certificaat, maar de oude controlleronderdelen worden tijdens herimplementatie van de nieuwe structuur geïsoleerd.

Optie C: Volledige systeemreconstructie. Biedt het hoogste niveau van beveiliging door een schone basislijn vast te stellen, hoewel dit de meest complexe aanpak is en een hoger risico op configuratiegerelateerde instabiliteit tijdens de wederopbouw met zich meebrengt. Dit is een langdurige optie en vereist expertise bij het opnieuw opbouwen van het sjabloon en de beleidsdatabases.

Zodra uw team deze opties heeft beoordeeld en de aanpak heeft geïdentificeerd die het beste aansluit bij uw risicomanagementnormen, laat het ons weten door op dit bericht te reageren. Na ontvangst van uw selectie, zullen wij het onderhoudsvenster coördineren en beginnen met de nodige technische voorbereidingen voor de uitvoering.

Wij stellen het op prijs dat u zich blijft richten op het onderhouden van een veilige netwerkinfrastructuur. Laat het ons weten als u verdere technische verduidelijking nodig hebt door deze e-mail te beantwoorden of via het bestaande serviceverzoek (SR) bij ons Technical Assistance Centre (TAC).

Met vriendelijke groet,
Cisco

Openen in Outlook

Gebruik de .eml download hieronder. Vervang alle [tussen haakjes geplaatste plaatsaanduidingen] vóór verzending.

✉ Open Outlook (alleen onderwerp)

↓ Download .eml Template

CloudOps 1 - Proactief - IoC gedetecteerd in Cloud Scan, Admin-Tech vereist om te valideren

Use case

Proactief verzonden wanneer een Cisco CloudOps-beveiligingsscan van een in de cloud gehoste SD-WAN-verbinding potentiële indicatoren van compromis (IoC's) heeft opgedoken. Er wordt namens de klant een SR geopend en de klant wordt gevraagd om admin-tech-bestanden bij te voegen, zodat de bevinding kan worden gevalideerd door middel van een volledige loganalyse.

onderwerp

Actie vereist: Admin-Tech-bestanden die nodig zijn om de bevindingen van de beveiligingsscan te valideren - SR [SR#]

bericht

Geachte klant,

Als onderdeel van onze voortdurende inzet voor het beveiligen en bewaken van de integriteit van Cisco-aanbiedingen, heeft Cisco onlangs een beveiligingsscan uitgevoerd van geselecteerde in de cloud gehoste SD-WAN-verbindingen. Deze actie werd ondernomen naar aanleiding van een gemeld veiligheidsprobleem. De scan heeft mogelijk verdachte activiteit in de structuur van uw organisatie geïdentificeerd die verdere beoordeling rechtvaardigt.

We vragen uw hulp om admin-tech-bestanden bij dit serviceverzoek (SR) te voegen, dat namens u is geopend, zodat we deze bevinding kunnen valideren en ons onderzoek kunnen voltooien.

Om een volledige analyse mogelijk te maken, kunt u admin-tech-bestanden verzamelen en uploaden van alle SD-WAN-besturingscomponenten. Zorg ervoor dat u zowel **"Logs"** als **"Tech"** selecteert bij het genereren van deze bestanden:

- **vSmarts (Controllers):** Verzamel één tegelijk, niet tegelijkertijd.
- **vBonds (Validators):** Verzamelen van alle knooppunten.
- **Beheer (vManage):** Verzamelen van alle knooppunten in het cluster (actieve en stand-by DR).

Voor gedetailleerde, stapsgewijze instructies voor het genereren en veilig indienen van uw admin-tech-bestanden, raadpleegt u deze handleiding: [Cisco SD-WAN Admin-Tech Collection Guide](#)^[1].

Zodra we de gevraagde bestanden hebben ontvangen, zal ons team ze analyseren om te bevestigen of de waargenomen activiteit een echte indicator van compromis vormt en u adviseren over de juiste volgende stappen.

Wij stellen het op prijs dat u zich blijft richten op het onderhouden van een veilige netwerkinfrastructuur. Laat het ons weten als u verdere technische verduidelijking nodig hebt door te reageren op dit serviceverzoek (SR).

Met vriendelijke groeten,
Cisco

Links:

[1] [Cisco SD-WAN Admin-Tech Collectiehandleiding](#)

Openen in Outlook

Gebruik de .eml download hieronder. Vervang alle **[tussen haakjes geplaatste plaatsaanduidingen]** vóór verzending.

✉ Open Outlook (alleen onderwerp)

↓ Download .eml Template

E-mails voor WAVE 2A voor klanten met een eerdere impact die de opties A, B of C nog niet hebben voltooid. (Opties 1 en 2 moeten opnieuw worden uitgevoerd)

TAC 9-sjabloon voor geen IOC voor PSIRT2a/zij herbouwd (EERDER GETROFFEN)

Use case

Verzonden naar klanten van wie de SD-WAN-logs **geen indicatoren van compromis (IoC's)** vertoonden met betrekking tot de

PSIRT2a-advisering EN die **eerder** hun fabric hebben **herbouwd**. Biedt bijgewerkte richtlijnen voor probleemoplossing met drie opties (vervolgoptie 2).

onderwerp

Dringende actie vereist: SD-WAN Infrastructure Critical Vulnerability Remediation – SR [SR#]

bericht

Geachte klant,

Bedankt dat u contact hebt opgenomen met het Cisco Technical Assistance Center (TAC) voor recente SD-WAN PSIRT-adviezen onder Serviceverzoek [SR#].

Na het bekijken van de logs en informatie van uw SD-WAN-verbinding, heeft onze analyse geen compromisindicatoren (IOC's) geïdentificeerd die verband houden met het SD-WAN-kwetsbaarheidsadvies van 5 juni 2026. Bovendien begrijpen we dat uw omgeving eerder een herbouw heeft ondergaan als onderdeel van herstelwerkzaamheden met betrekking tot eerdere adviezen.

We willen graag een belangrijke update delen met betrekking tot de aanbevolen richtlijnen voor het verhelpen van SD-WAN-verbindingen, rekening houdend met nieuw geïdentificeerde inzichten met betrekking tot deze kwetsbaarheden.

We bieden een kritische update voor de sanering van uw SD-WAN-verbinding, zoals vermeld in [SR #] en de eerder gecommuniceerde beveiligingsadviezen.

Hoewel u eerder een herstelplan hebt geselecteerd op basis van optie 2 — met een software-upgrade, herimplementatie van de controller en draaiing van SSH-sleutels — is onze analyse van het bedreigingslandschap blijven evolueren. Nieuwe technische inzichten met betrekking tot de exploitatie van deze kwetsbaarheden geven aan dat extra maatregelen dringend nodig zijn om het risico op persistentie te verminderen en de integriteit van de certificatenketen van vertrouwen te helpen waarborgen.

VEREISTE ACTIE:

We hebben de aanbevolen herstelstrategieën bijgewerkt om een uitgebreidere verdediging te bieden door aanvullende rotatie van rootcertificaten op te nemen.

Houd er rekening mee dat de herstelmaatregelen extra onderhoudsactiviteiten vereisen, waaronder geplande downtime van het netwerk. Aangezien de veiligheid en integriteit van uw netwerk onze prioriteit is, hebben we drie verschillende herstelopties ontwikkeld. Elke optie hieronder biedt een balans tussen operationele impact en beveiligingsgarantie voor uw overweging. Omdat uw interne risicohouding uniek is, kan Cisco geen bepaald pad aanbevelen.

Optie A: Herplaatsing met doorlopende herstart. Prioriteert operationele continuïteit door netwerkdowntime te vermijden, hoewel dit een resterend risico op dreigingspersistentie tijdens het overgangsproces met zich meebrengt.

Omschrijving: Omvat herimplementatie van de controller, plus SSH-sleutel en certificaatroteratie. Bestaande

controlleronderdelen worden tijdens de migratie via vManage verbonden om de nieuwe fabric te implementeren. Vervolgens worden ze verwijderd zodra het apparaat is gemigreerd.

Optie B: Herplaatsing met harde omslag. Biedt een hoger niveau van beveiliging. Omdat nieuwe controllers nooit verbinding maken met oude controllers, is er volledige isolatie. Dit heeft gevolgen voor de algemene netwerkactiviteiten, aangezien alle apparaten opnieuw verbinding moeten maken en route-/connectiviteitsinformatie moeten uitwisselen. Het tijdstip van uitval hangt af van het aantal sites, het aantal uitgewisselde voorvoegsels, enz.

Omschrijving: Omvat herimplementatie van de controller plus SSH-sleutel en rotatie van het certificaat, maar de oude controlleronderdelen worden tijdens herimplementatie van de nieuwe structuur geïsoleerd.

Optie C: Volledige systeemreconstructie. Biedt het hoogste niveau van beveiliging door een schone basislijn vast te stellen, hoewel dit de meest complexe aanpak is en een hoger risico op configuratiegerelateerde instabiliteit tijdens de wederopbouw met zich meebrengt. Dit is een langdurige optie en vereist expertise bij het opnieuw opbouwen van het sjabloon en de beleidsdatabases.

Zodra uw team deze opties heeft beoordeeld en de aanpak heeft geïdentificeerd die het beste aansluit bij uw risicomanagementnormen, laat het ons weten door op dit bericht te reageren. Na ontvangst van uw selectie, zullen wij het onderhoudsvenster coördineren en beginnen met de nodige technische voorbereidingen voor de uitvoering.

Wij stellen het op prijs dat u zich blijft richten op het onderhouden van een veilige netwerkinfrastructuur. Laat het ons weten als u verdere technische verduidelijking nodig hebt door deze e-mail te beantwoorden of via de bestaande serviceaanvraag.

Met vriendelijke groet,
Cisco

Openen in Outlook

Gebruik de .eml download hieronder. Vervang alle **[tussen haakjes geplaatste plaatsaanduidingen]** vóór verzending.

✉ Open Outlook (alleen onderwerp)

⬇ Download .eml Template

TAC 10-sjabloon voor ja IOC voor PSIRT2a / ze hebben opnieuw opgebouwd (EERDER BEÏNVLOED)

Use case

Verzonden naar klanten van wie de SD-WAN-logs **Indicators of Compromise (IoC's)** met betrekking tot het PSIRT2a-advies toonden EN die **eerder** hun fabric hebben **herbouwd**. Biedt bijgewerkte richtlijnen voor probleemoplossing met drie opties (vervolgoptie 2).

Geachte klant,

Bedankt dat u contact hebt opgenomen met het Cisco Technical Assistance Center (TAC) voor recente SD-WAN PSIRT-adviezen onder Serviceverzoek [SR#].

Na het analyseren van de logs die worden geleverd vanuit uw SD-WAN-verbinding, heeft ons team Indicators of Compromise (IOC's) geïdentificeerd die zijn gekoppeld aan het SD-WAN-kwetsbaarheidsadvies van 5 juni 2026. We begrijpen ook dat uw omgeving eerder een herbouw heeft ondergaan als onderdeel van saneringsstappen met betrekking tot eerdere adviezen.

We bieden een kritische update voor de sanering van uw SD-WAN-verbinding, zoals vermeld in [SR #] en de eerder gecommuniceerde beveiligingsadviezen. Deze update is specifiek voor stoffen waarin de verstrekte logboeken bewijs van compromisindicatoren (IOC's) vertoonden.

Hoewel u eerder een herstelplan hebt geselecteerd op basis van optie 2 — met een software-upgrade, herimplementatie van de controller en draaiing van SSH-sleutels — is onze analyse van het bedreigingslandschap blijven evolueren. Nieuwe technische inzichten met betrekking tot de exploitatie van deze kwetsbaarheden geven aan dat extra maatregelen dringend nodig zijn om het risico op persistentie te verminderen en de integriteit van de certificatenketen van vertrouwen te helpen waarborgen.

VEREISTE ACTIE:

We hebben de aanbevolen herstelstrategieën bijgewerkt om een uitgebreidere verdediging te bieden door aanvullende rotatie van rootcertificaten op te nemen.

Houd er rekening mee dat de herstelmaatregelen extra onderhoudsactiviteiten vereisen, waaronder geplande downtime van het netwerk. Aangezien de veiligheid en integriteit van uw netwerk onze prioriteit is, hebben we drie verschillende herstelopties ontwikkeld. Elke optie hieronder biedt een balans tussen operationele impact en beveiligingsgarantie voor uw overweging. Omdat uw interne risicohouding uniek is, kan Cisco geen bepaald pad aanbevelen.

Optie A: Herplaatsing met doorlopende herstart. Prioriteert operationele continuïteit door netwerkuptime te vermijden, hoewel dit een resterend risico op dreigingspersistentie tijdens het overgangsproces met zich meebrengt.

Omschrijving: Omvat herimplementatie van de controller, plus SSH-sleutel en certificaatrotatie. Bestaande controlleronderdelen worden tijdens de migratie via vManage verbonden om de nieuwe fabric te implementeren. Vervolgens worden ze verwijderd zodra het apparaat is gemigreerd.

Optie B: Herplaatsing met harde omslag. Biedt een hoger niveau van beveiliging. Omdat nieuwe controllers nooit verbinding maken met oude controllers, is er volledige isolatie. Dit heeft gevolgen voor de algemene netwerkactiviteiten,

aangezien alle apparaten opnieuw verbinding moeten maken en route-/connectiviteitsinformatie moeten uitwisselen. Het tijdstip van uitval hangt af van het aantal sites, het aantal uitgewisselde voorvoegsels, enz.

Omschrijving: Omvat herimplementatie van de controller plus SSH-sleutel en rotatie van het certificaat, maar de oude controlleronderdelen worden tijdens herimplementatie van de nieuwe structuur geïsoleerd.

Optie C: Volledige systeemreconstructie. Biedt het hoogste niveau van beveiliging door een schone basislijn vast te stellen, hoewel dit de meest complexe aanpak is en een hoger risico op configuratiegerelateerde instabiliteit tijdens de wederopbouw met zich meebrengt. Dit is een langdurige optie en vereist expertise bij het opnieuw opbouwen van het sjabloon en de beleidsdatabases.

Zodra uw team deze opties heeft beoordeeld en de aanpak heeft geïdentificeerd die het beste aansluit bij uw risicomanagementnormen, laat het ons weten door op dit bericht te reageren. Na ontvangst van uw selectie, zullen wij het onderhoudsvenster coördineren en beginnen met de nodige technische voorbereidingen voor de uitvoering.

Wij stellen het op prijs dat u zich blijft richten op het onderhouden van een veilige netwerkinfrastructuur. Laat het ons weten als u verdere technische verduidelijking nodig hebt door deze e-mail te beantwoorden of via de bestaande serviceaanvraag.

Met vriendelijke groet,
Cisco

Openen in Outlook

Gebruik de .eml download hieronder. Vervang alle **[tussen haakjes geplaatste plaatsaanduidingen]** vóór verzending.

✉ Open Outlook (alleen onderwerp)

↓ Download .eml Template

TAC 11 Template for no IOC for PSIRT2a/they did not rebuild (**EERDER GETROFFEN**)

Use case

Verzonden naar klanten van wie de SD-WAN-logs **geen indicatoren van compromis (IoC's)** vertoonden met betrekking tot de PSIRT2a-advisering EN die hun fabric **NIET opnieuw hebben opgebouwd**. Biedt bijgewerkte richtlijnen voor probleemoplossing met drie opties (vervolgoptie 1).

onderwerp

Dringende actie vereist: SD-WAN Infrastructure Critical Vulnerability Remediation – SR [SR#]

bericht

Geachte klant,

Bedankt dat u contact hebt opgenomen met het Cisco Technical Assistance Center (TAC) voor recente SD-WAN PSIRT-adviezen onder Serviceverzoek [SR#].

Na het bekijken van de logs en informatie die is verstrekt van uw SD-WAN-verbinding, hebben we geen Indicators of Compromise (IOC's) geïdentificeerd die zijn gekoppeld aan het SD-WAN-kwetsbaarheidsadvies van 5 juni 2026.

We begrijpen ook dat uw omgeving geen volledige herbouw heeft ondergaan na de vorige adviezen. Cisco raadt aan de bijgewerkte richtlijnen voor probleemoplossing hieronder te bekijken om potentiële blootstelling te verminderen en de integriteit van de SD-WAN-certificaatketen van vertrouwen te versterken.

Met dit in het achterhoofd bieden we een kritische update voor de sanering van uw SD-WAN-verbinding, zoals vermeld in [SR #] en de eerder gecommuniceerde beveiligingsadviezen.

Hoewel u eerder een herstelplan hebt geselecteerd op basis van optie 1 — met een software-upgrade en SSH-sleutelrotatie — is onze analyse van het dreigingslandschap blijven evolueren. Nieuwe technische inzichten met betrekking tot de exploitatie van deze kwetsbaarheden geven aan dat extra maatregelen dringend nodig zijn om het risico op persistentie te verminderen en de integriteit van de certificaatketen van vertrouwen te helpen waarborgen.

VEREISTE ACTIE:

We hebben de aanbevolen herstelstrategieën bijgewerkt om een uitgebreidere verdediging te bieden door aanvullende rotatie van rootcertificaten op te nemen.

Houd er rekening mee dat de herstelmaatregelen extra onderhoudsactiviteiten vereisen, waaronder geplande downtime van het netwerk. Aangezien de veiligheid en integriteit van uw netwerk onze prioriteit is, hebben we drie verschillende herstelopties ontwikkeld. Elke optie hieronder biedt een balans tussen operationele impact en beveiligingsgarantie voor uw overweging. Omdat uw interne risicohouding uniek is, kan Cisco geen bepaald pad aanbevelen.

Optie A: Herplaatsing met doorlopende herstart. Prioriteert operationele continuïteit door netwerkdowntime te vermijden, hoewel dit een resterend risico op dreigingspersistentie tijdens het overgangsproces met zich meebrengt.

Omschrijving: Omvat herimplementatie van de controller, plus SSH-sleutel en certificaatrotatie. Bestaande controlleronderdelen worden tijdens de migratie via vManage verbonden om de nieuwe fabric te implementeren. Vervolgens worden ze verwijderd zodra het apparaat is gemigreerd.

Optie B: Herplaatsing met harde omslag. Biedt een hoger niveau van beveiliging. Omdat nieuwe controllers nooit verbinding maken met oude controllers, is er volledige isolatie. Dit heeft gevolgen voor de algemene netwerkactiviteiten, aangezien alle apparaten opnieuw verbinding moeten maken en route-/connectiviteitsinformatie moeten uitwisselen. Het tijdstip van uitval hangt af van het aantal sites, het aantal uitgewisselde voorvoegsels, enz.

Omschrijving: Omvat herimplementatie van de controller plus SSH-sleutel en rotatie van het certificaat, maar de oude

controlleronderdelen worden tijdens herimplementatie van de nieuwe structuur geïsoleerd.

Optie C: Volledige systeemreconstructie. Biedt het hoogste niveau van beveiliging door een schone basislijn vast te stellen, hoewel dit de meest complexe aanpak is en een hoger risico op configuratiegerelateerde instabiliteit tijdens de wederopbouw met zich meebrengt. Dit is een langdurige optie en vereist expertise bij het opnieuw opbouwen van het sjabloon en de beleidsdatabases.

Zodra uw team deze opties heeft beoordeeld en de aanpak heeft geïdentificeerd die het beste aansluit bij uw risicomanagementnormen, laat het ons weten door op dit bericht te reageren. Na ontvangst van uw selectie, zullen wij het onderhoudsvenster coördineren en beginnen met de nodige technische voorbereidingen voor de uitvoering.

Wij stellen het op prijs dat u zich blijft richten op het onderhouden van een veilige netwerkinfrastructuur. Laat het ons weten als u verdere technische verduidelijking nodig hebt door deze e-mail te beantwoorden of via de bestaande serviceaanvraag.

Met vriendelijke groet,
Cisco

Openen in Outlook

Gebruik de .eml download hieronder. Vervang alle [tussen haakjes geplaatste plaatsaanduidingen] vóór verzending.

✉ Open Outlook (alleen onderwerp)

↓ Download .eml Template

TAC 12 Template for yes IOC for PSIRT2a/they did not rebuild (**EERDER GETROFFEN**)

Use case

Verzonden naar klanten van wie de SD-WAN-logs **Indicators of Compromise (IoC's)** met betrekking tot het PSIRT2a-advies toonden EN die hun fabric **NIET opnieuw hebben opgebouwd**. Biedt bijgewerkte richtlijnen voor probleemoplossing met drie opties (vervolgoptie 1).

onderwerp

Dringende actie vereist: SD-WAN Infrastructure Critical Vulnerability Remediation – SR [SR#]

bericht

Geachte klant,

Bedankt dat u contact hebt opgenomen met het Cisco Technical Assistance Center (TAC) voor recente SD-WAN PSIRT-

adviezen onder Serviceverzoek [SR#].

Na het analyseren van de logs die worden geleverd vanuit uw SD-WAN-verbinding, heeft ons team Indicators of Compromise (IOC's) geïdentificeerd die zijn gekoppeld aan het SD-WAN-kwetsbaarheidsadvies van 5 juni 2026. Bovendien begrijpen we dat uw omgeving geen volledige herbouw heeft ondergaan na eerdere adviezen.

Gezien de aanwezigheid van deze indicatoren en het evoluerende inzicht in het dreigingslandschap, is het belangrijk om de hieronder geschetste bijgewerkte remediëringsrichtlijnen te herzien en te implementeren om het risico op persistentie te verminderen en de integriteit van uw SD-WAN-certificaatketen van vertrouwen te waarborgen.

We bieden een kritische update voor de sanering van uw SD-WAN-verbinding, zoals vermeld in [SR #] en de eerder gecommuniceerde beveiligingsadviezen. Deze update is specifiek voor stoffen waarin de verstrekte logboeken bewijs van compromisindicatoren (IOC's) vertoonden.

Hoewel u eerder een herstelplan hebt geselecteerd op basis van optie 1 — met een software-upgrade en SSH-sleutelrotatie — is onze analyse van het dreigingslandschap blijven evolueren. Nieuwe technische inzichten met betrekking tot de exploitatie van deze kwetsbaarheden geven aan dat extra maatregelen dringend nodig zijn om het risico op persistentie te verminderen en de integriteit van de certificaatketen van vertrouwen te helpen waarborgen.

VEREISTE ACTIE:

We hebben de aanbevolen herstelstrategieën bijgewerkt om een uitgebreidere verdediging te bieden door aanvullende rotatie van rootcertificaten op te nemen.

Houd er rekening mee dat de herstelmaatregelen extra onderhoudsactiviteiten vereisen, waaronder geplande downtime van het netwerk. Aangezien de veiligheid en integriteit van uw netwerk onze prioriteit is, hebben we drie verschillende herstelopties ontwikkeld. Elke optie hieronder biedt een balans tussen operationele impact en beveiligingsgarantie voor uw overweging. Omdat uw interne risicohouding uniek is, kan Cisco geen bepaald pad aanbevelen.

Optie A: Herplaatsing met doorlopende herstart. Prioriteert operationele continuïteit door netwerkdowntime te vermijden, hoewel dit een resterend risico op dreigingspersistentie tijdens het overgangsproces met zich meebrengt.

Omschrijving: Omvat herimplementatie van de controller, plus SSH-sleutel en certificaatrotatie. Bestaande controlleronderdelen worden tijdens de migratie via vManage verbonden om de nieuwe fabric te implementeren. Vervolgens worden ze verwijderd zodra het apparaat is gemigreerd.

Optie B: Herplaatsing met harde omslag. Biedt een hoger niveau van beveiliging. Omdat nieuwe controllers nooit verbinding maken met oude controllers, is er volledige isolatie. Dit heeft gevolgen voor de algemene netwerkactiviteiten, aangezien alle apparaten opnieuw verbinding moeten maken en route-/connectiviteitsinformatie moeten uitwisselen. Het tijdstip van uitval hangt af van het aantal sites, het aantal uitgewisselde voorvoegsels, enz.

Omschrijving: Omvat herimplementatie van de controller plus SSH-sleutel en rotatie van het certificaat, maar de oude

controlleronderdelen worden tijdens herimplementatie van de nieuwe structuur geïsoleerd.

Optie C: Volledige systeemreconstructie. Biedt het hoogste niveau van beveiliging door een schone basislijn vast te stellen, hoewel dit de meest complexe aanpak is en een hoger risico op configuratiegerelateerde instabiliteit tijdens de wederopbouw met zich meebrengt. Dit is een langdurige optie en vereist expertise bij het opnieuw opbouwen van het sjabloon en de beleidsdatabases.

Zodra uw team deze opties heeft beoordeeld en de aanpak heeft geïdentificeerd die het beste aansluit bij uw risicomanagementnormen, laat het ons weten door op dit bericht te reageren. Na ontvangst van uw selectie, zullen wij het onderhoudsvenster coördineren en beginnen met de nodige technische voorbereidingen voor de uitvoering.

Wij stellen het op prijs dat u zich blijft richten op het onderhouden van een veilige netwerkinfrastructuur. Laat het ons weten als u verdere technische verduidelijking nodig hebt door deze e-mail te beantwoorden of via de bestaande serviceaanvraag.

Met vriendelijke groet,
Cisco

Openen in Outlook

Gebruik de .eml download hieronder. Vervang alle [tussen haakjes geplaatste plaatsaanduidingen] vóór verzending.

✉ Open Outlook (alleen onderwerp)

↓ Download .eml Template

E-mails voor WAVE 2A voor nieuwe klanten (niet eerder beïnvloed)

TAC 13 Template for no IOC / No Fixed Release Available (WAVE 2a — Await Fix)

Use case

Verzonden naar klanten waarvan de SD-WAN-logs **geen indicatoren van compromis (IoC's)** vertoonden met betrekking tot CVE-2026-20245, maar voor wie **momenteel geen vaste softwarerelease beschikbaar is** voor hun platform / versie. Adviseert de klant om tussentijdse verhardingsmaatregelen toe te passen en te wachten op de melding van de vaste release.

onderwerp

Update: IoC-evaluatie voltooid voor CVE-2026-20245 – momenteel geen vaste release beschikbaar – SR [SR#]

bericht

Geachte klant,

Bedankt dat u contact hebt opgenomen met het Cisco Technical Assistance Center (TAC) voor CVE-2026-20245 onder Serviceverzoek [SR#].

We hebben de analyse van de admin-tech-bestanden die u hebt verstrekt van uw SD-WAN-besturingscomponenten voltooid. **In de onderzochte logboeken hebben we geen aan CVE-2026-20245 gerelateerde indicatoren van compromissen (IoC's) vastgesteld.**

Houd er rekening mee dat de hoeveelheid logboekgegevens die voor deze beoordeling zijn opgehaald en aan Cisco zijn verstrekt, mogelijk is beperkt door de logboekbewaarperiode die in uw omgeving is geconfigureerd volgens de [Cisco SD-WAN Hardening Guide](#)^[1].

BELANGRIJK — Er is momenteel geen vaste softwarerelease beschikbaar:

Op dit moment is er **geen vaste softwarerelease beschikbaar** voor uw huidige platform- en softwareversie om dit beveiligingslek te verhelpen. Cisco engineering werkt actief aan een vaste release. Zodra de vaste software beschikbaar is, wordt het [officiële veiligheidsadvies](#)^[2] bijgewerkt met de informatie over de vaste release.

Aanbevolen tussentijdse acties:

In afwachting van de vaste release, raden we ten eerste aan de volgende verhardingsmaatregelen te implementeren om uw blootstelling te verminderen:

1. **Best practices voor harden toepassen:** bekijk en implementeer de aanbevelingen in de [Cisco SD-WAN Hardening Guide](#)^[1] om het aanvalsoppervlak te verkleinen.
2. **Monitor de Security Advisory:** Controleer periodiek de [officiële security advisory](#)^[2] voor updates over de beschikbaarheid van vaste releases voor uw platform.
3. **Plan voor upgrade:** Begin nu met uw upgradeplanning zodat u klaar bent om de upgrade onmiddellijk uit te voeren zodra de vaste release is gepubliceerd.
4. **Bewaak uw omgeving:** blijf uw SD-WAN-besturingscomponenten controleren op afwijkend gedrag of onverwachte configuratiewijzigingen.

Volgende stappen:

We zullen deze zaak bijwerken wanneer de vaste softwarerelease beschikbaar komt. Op dat moment moet u prioriteit geven aan de upgrade van alle SD-WAN-besturingscomponenten (Manager, Controller, Validator) naar de vaste versie zo snel mogelijk.

Als u een BCS/LCS-abonnement hebt, neemt u contact op met uw Cisco NCE of Delivery Manager voor meer informatie over upgradeplanning.

Wij waarderen uw geduld en uw inzet voor de veiligheid van uw infrastructuur. Als u vragen hebt of tussentijds verdere hulp nodig hebt, aarzel dan niet om op deze zaak te reageren.

Met vriendelijke groeten,

Cisco Technical Assistance Centre (TAC)

Links:

[1] [Cisco SD-WAN Hardening Guide](#)

[2] [Officiële veiligheidsadviseur \(cisco-sa-sdwan-privesc-4uxFRDZX\)](#)

Openen in Outlook

Vervang alle *[tussen haakjes geplaatste plaatsaanduidingen]* vóór verzending.

✉ Open Outlook (alleen onderwerp)

⬇ Download .eml Template

TAC 14 Template for no IOC / Fixed Release Available (WAVE 2a — Upgrade Now)

Use case

Verzonden naar klanten waarvan de SD-WAN-logs **geen Indicators of Compromise (IoC's)** vertoonden met betrekking tot CVE-2026-20245 EN voor wie een **vaste softwarerelease beschikbaar is**. Adviseert de klant om onmiddellijk door te gaan met het plannen en uitvoeren van upgrades.

onderwerp

Update: IoC-evaluatie voltooid voor CVE-2026-20245 - geen IoC's gevonden, upgrade vereist - SR [SR#]

bericht

Geachte klant,

Bedankt dat u contact hebt opgenomen met het Cisco Technical Assistance Center (TAC) voor CVE-2026-20245 onder Serviceverzoek [SR#].

We hebben de analyse van de admin-tech-bestanden die u hebt verstrekt van uw SD-WAN-besturingscomponenten voltooid. **In de onderzochte logboeken hebben we geen** aan CVE-2026-20245 gerelateerde **indicatoren van compromissen (IoC's)** vastgesteld.

Houd er rekening mee dat de hoeveelheid logboekgegevens die voor deze beoordeling zijn opgehaald en aan Cisco zijn verstrekt, mogelijk is beperkt door de logboekbewaarperiode die in uw omgeving is geconfigureerd volgens de [Cisco SD-WAN Hardening Guide](#)^[1].

Belangrijk — Upgrade vereist:

Hoewel er geen IoC's zijn geïdentificeerd, blijft de onderliggende kwetsbaarheid aanwezig totdat uw SD-WAN-besturingscomponenten zijn geüpgraded naar een vaste softwarerelease. Er is nu een vaste release beschikbaar voor uw platform.

Geef **prioriteit aan uw upgradeplanning en -uitvoering** als de meest kritieke stap om deze kwetsbaarheid te verhelpen. Als u deze upgrade nog niet hebt gepland, moet u dit onmiddellijk doen.

Volgende stappen:

1. **Upgrade alle SD-WAN-besturingscomponenten:** Upgrade uw Manager (vManage), Controller (vSmart) en Validator (vBond) naar een vaste softwareversie die wordt vermeld in het [officiële beveiligingsadvies](#)^[2].
2. **Upgradebronnen:** raadpleeg de volgende officiële Cisco-documenten voor gedetailleerde upgradeinstructies:
 - [Start uw Catalyst SD-WAN-upgrade](#)^[3]
 - [Cisco SD-WAN-upgradehandleiding](#)^[4]
3. **Sluiting van kwestie:** nadat u de software-upgrade in uw omgeving met succes hebt voltooid, kunt u deze kwestie als opgelost beschouwen en doorgaan met de standaardprocedures voor sluiting.

Als u een BCS/LCS-abonnement hebt, neemt u contact op met uw Cisco NCE of Delivery Manager voor meer informatie over het upgradeproces.

Wij zullen uw zaak blijven volgen. Als we niet binnen 10 werkdagen terughoren, gaan we ervan uit dat er geen verdere hulp nodig is en gaan we verder met de normale procedures voor de sluiting van de TAC-zaak.

Met vriendelijke groeten,
Cisco Technical Assistance Centre (TAC)

Links:

- [1] [Cisco SD-WAN Hardening Guide](#)
- [2] [Officiële veiligheidsadviseur \(cisco-sa-sdwan-privesc-4uxFRDZX\)](#)
- [3] [Start uw Catalyst SD-WAN-upgrade](#)
- [4] [Upgradehandleiding voor Cisco SD-WAN](#)

Openen in Outlook

Vervang alle **[tussen haakjes geplaatste plaatsaanduidingen]** vóór verzending.

✉ Open Outlook (alleen onderwerp)

⬇ Download .eml Template

dringende upgrade)

Use case

Verzonden naar klanten waarvan de SD-WAN-logs **Indicators of Compromise (IoC's)** met betrekking tot CVE-2026-20245 toonden EN voor wie een **vaste softwarerelease beschikbaar is**. Adviseert de klant om dringend te upgraden en een beoordelingsgesprek in te plannen om bevindingen en herstel te bespreken.

onderwerp

URGENT: IoC geïdentificeerd voor CVE-2026-20245 – Onmiddellijke upgrade vereist – SR [SR#]

bericht

Geachte klant,

Bedankt dat u contact hebt opgenomen met het Cisco Technical Assistance Center (TAC) voor CVE-2026-20245 onder Serviceverzoek [SR#].

Na analyse van de admin-tech bestanden die worden geleverd door uw SD-WAN-besturingscomponenten, heeft ons team **Indicators of Compromise (IoC's)** geïdentificeerd die zijn gekoppeld aan CVE-2026-20245.

Gezien de aard van deze bevindingen is het van cruciaal belang dat we de technische details en de aanbevolen volgende stappen zo snel mogelijk bespreken. We willen graag een gesprek met uw team plannen om de specifieke bevindingen te bekijken en het juiste herstelpad te bespreken.

Onmiddellijke acties vereist:

1. **Upgrade SD-WAN-besturingscomponenten onmiddellijk:** een vaste softwarerelease is beschikbaar voor uw platform. Upgrade uw Manager (vManage), Controller (vSmart) en Validator (vBond) naar een vaste softwareversie die zo snel mogelijk wordt vermeld in de [officiële beveiligingsadvies](#)^[1]. De upgrade sluit de kwetsbaarheid onmiddellijk af.
2. **Plan een Review Call:** Laat ons uw beschikbaarheid voor een kort gesprek binnen de volgende [bijv. 4-8 uur] weten om de IoC-bevindingen te bekijken en de aanbevolen herstelopties te bespreken.
3. **Best practices voor harden toepassen:** bekijk en implementeer de aanbevelingen in de [Cisco SD-WAN Hardening Guide](#)^[2] om het aanvalsoppervlak te verminderen terwijl sanering is gepland.

Upgradebronnen:

- [Start uw Catalyst SD-WAN-upgrade](#)^[3]
- [Cisco SD-WAN-upgradehandleiding](#)^[4]

Belangrijk: na de upgrade kunnen aanvullende herstelstappen (zoals het opnieuw implementeren van de controller en het draaien van het certificaat) worden aanbevolen, afhankelijk van de ernst van het vastgestelde compromis. Deze

zullen worden besproken tijdens de oproep tot herziening.

Raadpleeg ook de [TAC-remediëringsgids](#)^[5] voor gedetailleerde herstelopties.

Ons primaire doel is om u te helpen bij het beveiligen van uw omgeving en het beperken van mogelijke risico's. Wij waarderen uw snelle aandacht voor deze zaak en kijken ernaar uit om met u te coördineren.

Met vriendelijke groeten,

Cisco Technical Assistance Centre (TAC)

Links:

[1] [Officiële veiligheidsadviseur \(cisco-sa-sdwan-privesc-4uxFRDZX\)](#)

[2] [Cisco SD-WAN Hardening Guide](#)

[3] [Start uw Catalyst SD-WAN-upgrade](#)

[4] [Upgradehandleiding voor Cisco SD-WAN](#)

[5] [Handleiding voor TAC-sanering](#)

Openen in Outlook

Vervang alle *[tussen haakjes geplaatste plaatsaanduidingen]* vóór verzending.

✉ Open Outlook (alleen onderwerp)

⬇ Download .eml Template

TAC 16 Template for IOC Identified / No Fixed Release Available (WAVE 2a — Harden & Await Fix)

Use case

Verzonden naar klanten waarvan de SD-WAN-logs **Indicators of Compromise (IoC's)** met betrekking tot CVE-2026-20245 toonden, maar voor wie **momenteel geen vaste software release beschikbaar is** voor hun platform / versie. Adviseert onmiddellijke verharding, plant een beoordelingsgesprek en informeert de klant dat ze moeten wachten tot de vaste release volledig is verholpen.

onderwerp

URGENT: IoC geïdentificeerd voor CVE-2026-20245 - geen vaste release momenteel beschikbaar - SR [SR#]

bericht

Geachte klant,

Bedankt dat u contact hebt opgenomen met het Cisco Technical Assistance Center (TAC) voor CVE-2026-20245 onder

Serviceverzoek [SR#].

Na analyse van de admin-tech bestanden die worden geleverd door uw SD-WAN-besturingscomponenten, heeft ons team **Indicators of Compromise (IoC's)** geïdentificeerd die zijn gekoppeld aan CVE-2026-20245.

Gezien de ernst van deze bevindingen is het van cruciaal belang dat we de technische details en de aanbevolen tussentijdse maatregelen zo snel mogelijk bespreken. We willen graag een gesprek met uw team plannen om de specifieke bevindingen te bekijken.

BELANGRIJK — Er is momenteel geen vaste softwarerelease beschikbaar:

Op dit moment is er **geen vaste softwarerelease beschikbaar** voor uw huidige platform- en softwareversie om deze kwetsbaarheid volledig te verhelpen. Cisco engineering werkt actief aan een vaste release. Zodra de vaste software beschikbaar is, wordt het [officiële veiligheidsadvies](#)^[1] bijgewerkt met de informatie over de vaste release.

Onmiddellijke acties vereist:

1. **Plan een Review Call:** Laat ons weten dat u binnen de volgende [bijv. 4-8 uur] beschikbaar bent voor een kort gesprek om de IoC-bevindingen te bekijken en tussentijdse inperkingsmaatregelen te bespreken.
2. **Pas de best practices voor harden onmiddellijk toe:** bekijk en implementeer de aanbevelingen in de [Cisco SD-WAN Hardening Guide](#)^[2] om het aanvalsoppervlak te verkleinen in afwachting van de vaste release.
3. **Verhoogde bewaking:** houd uw SD-WAN-besturingscomponenten nauwlettend in de gaten voor afwijkend gedrag, onverwachte configuratiewijzigingen of ongeoorloofde toegangspogingen.
4. **Monitor de Security Advisory:** Controleer periodiek de [officiële security advisory](#)^[1] voor updates over de beschikbaarheid van vaste releases voor uw platform.
5. **Plan voor upgrade:** Begin nu met uw upgradeplanning zodat u klaar bent om de upgrade onmiddellijk uit te voeren zodra de vaste release is gepubliceerd.

Volgende stappen:

We zullen deze zaak bijwerken wanneer de vaste softwarerelease beschikbaar komt. Op dat moment moet u prioriteit geven aan de upgrade van alle SD-WAN-besturingscomponenten (Manager, Controller, Validator) naar de vaste versie onmiddellijk. Na de upgrade zullen aanvullende herstelstappen (zoals het opnieuw implementeren van de controller en het roteren van het certificaat) worden besproken op basis van de bevindingen die tijdens ons gesprek zijn beoordeeld.

Zie ook de [TAC-remediëringsgids](#)^[3] voor informatie over herstelopties die van toepassing zullen zijn zodra de vaste release beschikbaar komt.

Ons primaire doel is om u te helpen bij het beveiligen van uw omgeving en het beperken van mogelijke risico's. Wij waarderen uw snelle aandacht voor deze zaak en kijken ernaar uit om met u te coördineren.

Met vriendelijke groeten,
Cisco Technical Assistance Centre (TAC)

Links:

- [1] [Officiële veiligheidsadviseur \(cisco-sa-sdwan-privesc-4uxFRDZX\)](#)
- [2] [Cisco SD-WAN Hardening Guide](#)
- [3] [Handleiding voor TAC-herstel](#)

Openen in Outlook

Vervang alle **[tussen haakjes geplaatste plaatsaanduidingen]** vóór verzending.

✉ Open Outlook (alleen onderwerp)

↓ Download .eml Template

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.