

Auf bereits vorhandene Artikel fett markieren

Inhalt

[Einleitung](#)

[Referenzen - Cisco SD-WAN CVE-2026-20182-Dokumentation](#)

[E-Mails](#)

[Sherlock 1 - Einlass - Upgrade- und Admin-Tech-Dateien anfordern](#)

[Sherlock 2 - Ergebnis - Keine IoCs beobachtet \(pro Datei\)](#)

[Sherlock 3 - Erinnerung - Admin-Tech-Dateien fehlen](#)

[TAC 1 - Untersuchung - weitere Überprüfung erforderlich \(IoC-Verdacht\)](#)

[TAC 2 - Ergebnis - Keine IoCs gefunden \(vom Techniker bestätigt\)](#)

[TAC 3 - Validierung - IP-Eigentumsrechte an Overlay bestätigen](#)

[TAC 4 - Ergebnis - Falsch positiv geklärt](#)

[TAC 5 - Kritisch - IoC identifiziert, Zeitplan Überprüfung Anruf](#)

[TAC 6 - Ergebnis - Doppeltes IoC \(Schließen und Umleiten\)](#)

[TAC 7 - Problembehebung - Follow-up-Optionen \(nach Anruf\)](#)

[TAC 8 - Problembehebung - Aktualisierte Optionen für kompromittierte Strukturen \(Option 2\)](#)

[TAC 17 - Reversed Finding - früher kein IoC, jetzt IoC identifiziert \(CVE-2026-20182\)](#)

[CloudOps 1 - Proaktiv - IoC beim Cloud-Scan erkannt, Admin-Tech zur Validierung erforderlich](#)

[E-Mails für WAVE 2A für ZUVOR BETROFFENE Kunden, die die Optionen A, B ODER C noch nicht abgeschlossen haben \(die Optionen 1 und 2 müssen erneut durchgeführt werden\)](#)

[TAC 9-Vorlage ohne IOC für PSIRT2a/Neuaufbau \(VORHER AUSGEFÜHRT\)](#)

[TAC 10 Vorlage für yes IOC für PSIRT2a/they did rebuild \(PREVIOUSLY IMPACTED\)](#)

[TAC 11-Vorlage ohne IOC für PSIRT2a/wurde nicht neu erstellt \(ZUVOR AUSGEFÜHRT\)](#)

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

[E-Mails für WAVE 2A für NEUE Kunden \(bisher nicht betroffen\)](#)

[TAC 13-Vorlage für kein IOC/kein festes Release verfügbar \(WAVE 2a — Wartet auf Lösung\)](#)

[TAC 14-Vorlage ohne IOC/Fixed Release verfügbar \(WAVE 2a - Jetzt aktualisieren\)](#)

[TAC 15-Vorlage für identifizierte/feste IOC-Version verfügbar \(WAVE 2a — dringendes Upgrade\)](#)

[TAC 16-Vorlage für IOC identifiziert/keine feste Version verfügbar \(WAVE 2a — Harden & Await Fix\)](#)

Einleitung

In diesem Dokument werden die genehmigten E-Mail-Vorlagen für Kunden zentralisiert, die bei der Triage und der Behebung von Fällen verwendet werden, die mit der Authentifizierungs-Bypass-Schwachstelle des Cisco Catalyst SD-WAN-Controllers in Zusammenhang stehen. Die Vorlagen werden nach Absender aufgeteilt: Sherlock (automatisierter Fallaustausch, bei dem Daten aus dem Admin-Tech-Bereich gesammelt werden und vorläufige IoC-Ergebnisse zurückgegeben werden) und TAC-Techniker (vom Menschen gesteuerte Follow-ups für

Untersuchungen, Validierungen und Anleitungen zur Problembehebung).

Referenzen - Cisco SD-WAN CVE-2026-20182-Dokumentation

Eine Master-Liste aller Cisco Dokumente, auf die in den obigen E-Mail-Vorlagen verwiesen wird. Die Nummerierung ist einheitlich - hochgestellt per E-Mail (z.B. ^[2]) Zeigen Sie auf die Artikel in dieser Liste.

1. **Cisco SD-WAN Hardening Guide:** <https://sec.cloudapps.cisco.com/security/center/resources/Cisco-Catalyst-SD-WAN-HardeningGuide>
2. **Official Security Advisory (cisco-sa-sdwan-mltnps2-JxpWm7R) -**
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-mltnps2-JxpWm7R>
3. **TAC-Sanierungsleitfaden:** <https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/225842-remediate-catalyst-sd-wan-security.html#toc-h1d--1516256622>
4. **Cisco SD-WAN-Upgrade-Leitfaden:** <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. **Second Security Advisory (cisco-sa-sdwan-rpa2-v69WY2SW) -**
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa2-v69WY2SW>
7. **Starten Sie Ihr Catalyst SD-WAN-Upgrade -** <https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/225515-start-your-catalyst-sd-wan-upgrade.html>

E-Mails

Sherlock 1 - Einlass - Upgrade- und Admin-Tech-Dateien anfordern

Anwendungsfall

Erste Kontaktaufnahme bei Eröffnung eines TAC-Tickets für CVE-2026-20182 mit Rat und Tat zur Erfassung admin-tech-Daten von und dann zur Aktualisierung aller SD-WAN-Steuerungskomponenten.

Betreff

Wichtig: Maßnahme erforderlich für CVE-2026-20182 - Upgrade-Planung und IoC-Analyse

Nachricht

Sehr geehrter Kunde,

Vielen Dank, dass Sie sich an das Cisco Technical Assistance Center (TAC) wenden.

In Bezug auf die Schwachstelle im Zusammenhang mit **CVE-2026-20182** lesen Sie bitte die [offizielle Sicherheitsempfehlung](#)^[1] für vollständige Details sowie den [TAC-Remediation-Leitfaden](#)^[2].

Unser vorrangiges Ziel ist es, Ihre Umgebung zu schützen. **Priorisieren Sie Ihre Upgrade-Planung und -Durchführung** als wichtigsten Schritt zur Minderung dieses Risikos. Wenn Sie dieses Upgrade noch nicht geplant haben, führen Sie es bitte sofort durch.

Upgrade-Ressourcen: Detaillierte Anweisungen zur Durchführung des Upgrades finden Sie im folgenden offiziellen Dokument von Cisco: [Cisco SD-WAN-Upgrade-Leitfaden](#)^[3]

Um eine erste Bewertung Ihrer Umgebung hinsichtlich potenzieller Indicators of Compromise (IoCs) im Zusammenhang mit CVE-2026-20182 zu ermöglichen, müssen Sie *vor dem* Upgrade eine Sammlung von Admin-Tech-Informationen durchführen. Befolgen Sie die folgende Reihenfolge:

- 1. Admin-Tech-Dateien sammeln:** Generieren Sie vor dem Upgrade die Admin-Tech-Protokolle aller SD-WAN-Steuerungskomponenten, um sicherzustellen, dass keine Diagnosedaten verloren gehen. Wählen Sie beim Generieren dieser Dateien sowohl **"Protokolle"** als auch **"Technik"** aus.
 - **vSmarts (Controller):** Sammeln Sie eine nach der anderen, nicht gleichzeitig.
 - **vBonds (Prüfer):** Von allen Knoten sammeln.
 - **Manager (vManage):** Sammeln Sie alle Knoten im Cluster (Active und Standby-DR).
- 2. Upgrade ausführen:** Aktualisieren Sie alle SD-WAN-Steuerungskomponenten (vManage, vSmart, vBond) auf eine feste Softwareversion, die in der Ankündigung aufgeführt ist. Warten Sie nicht auf die Analyse des Admin-Tech-Protokolls, bevor Sie mit dem Upgrade beginnen, da das Upgrade die Schwachstelle sofort schließt.
- 3. Hochladen zu TAC-Ticket:** Laden Sie nach Abschluss des Upgrades die zuvor erfassten Dateien, wenn möglich, gleichzeitig in Ihren vorhandenen TAC-Ticket hoch. Anschließend führt unser Team eine Überprüfung dieser Protokolle durch, um Ihre Umgebung auf Indicators of Compromise (IoCs) zu überprüfen.

Ressourcen und Support:

Weitere Details und schrittweise Anleitungen zum Erstellen und sicheren Senden von Admin-Tech-Dateien finden Sie in diesem Handbuch: [Cisco SD-WAN Admin-Tech Collection-Leitfaden](#)^[4].

Wenn Sie ein BCS/LCS-Abonnement haben, wenden Sie sich an Ihren Cisco NCE oder Delivery Manager, um weitere Unterstützung beim Upgrade-Prozess oder den nächsten Schritten zu erhalten.

Datenschutz und Sicherheit bleiben für uns oberste Priorität. Alle bereitgestellten Informationen werden in Übereinstimmung mit den Datenschutz- und Sicherheitsrichtlinien von Cisco behandelt.

Sie erhalten eine automatische E-Mail-Bestätigung für **JEDE** erfolgreich in das Ticket hochgeladene Datei. Bitte überprüfen Sie diese Benachrichtigungen.

Vielen Dank für Ihre schnelle Zusammenarbeit bei der Sicherung Ihrer Infrastruktur.

Links:

[1] [Offizielles Sicherheitshinweis](#)

[2] [TAC-Sanierungsleitfaden](#)

[3] [Cisco SD-WAN-Upgrade-Leitfaden](#)

[4] [Cisco SD-WAN Admin-Tech Collection-Leitfaden](#)

Mit freundlichen Grüßen

In Outlook öffnen

① Verwenden Sie die .eml-Download unten. Ersetzen Sie alle **[Platzhalter in Klammern]** vor dem Senden.

✉ Outlook öffnen (nur Betreff)

⬇ EML-Vorlage herunterladen

Sherlock 2 - Ergebnis - Keine IoCs beobachtet (pro Datei)

Anwendungsfall

Wird nach einer Administrator-technischen Analyse gesendet, werden für eine bestimmte hochgeladene Datei keine Anzeichen für eine Kompromittierung beobachtet. Einmal pro verarbeiteter Datei gesendet.

Betreff

Update: Analyseergebnisse für SD-WAN-Komponente [Dateinamen einfügen] - CVE-2026-20182

Nachricht

Sehr geehrter Kunde,

Vielen Dank für Ihre Geduld.

Wir haben die Analyse der admin-tech-Datei [Dateiname einfügen] abgeschlossen. In dieser Datei wurden keine Anzeichen für eine Kompromittierung im Zusammenhang mit CVE-2026-20182 für dieses spezielle Gerät identifiziert.

Bitte beachten Sie, dass die Menge der von Ihnen abgerufenen und an Cisco für diese Überprüfung bereitgestellten Protokolldaten möglicherweise durch die Protokollaufbewahrungszeit begrenzt wurde, die Sie gemäß dem **Cisco SD-WAN Hardening Guide** [¹] konfiguriert haben.

Wichtig: Nächste Schritte und Ticketabschluss:

1. **Auf alle Ergebnisse warten:** Beachten Sie, dass diese E-Mail möglicherweise nur Teilergebnisse enthält. Wir analysieren jede Datei, wie sie bereitgestellt wird. Warten Sie, bis Sie eine Bestätigung für alle hochgeladenen Dateien erhalten haben, bevor Sie die Umfrage als abgeschlossen betrachten.
2. **Upgrade-Priorität:** Während die ersten Scans von Admin-Tech-Protokollen noch keine Indications of Compromise (IoCs) identifiziert haben, bleibt die zugrunde liegende Schwachstelle möglicherweise bestehen. Falls noch nicht geschehen, priorisieren Sie bei Cisco Cloud-Pro- und Cisco On-Prem-Bereitstellungen so bald wie möglich das vollständige Upgrade Ihrer SD-WAN-Steuerungskomponenten.
 - Cisco Cloud (fka: SaaS) Customer Fabrics werden von Cisco im Rahmen des Managed Service automatisch aktualisiert. Keine Aktion erforderlich.
3. **Ticketabschluss:** Sobald Sie für alle hochgeladenen Dateien die Meldung "No Observed IoC" (Kein IoC beobachtet) erhalten UND (falls zutreffend) das Software-Upgrade in Ihrer Umgebung erfolgreich abgeschlossen haben, können Sie diesen Fall als gelöst betrachten und mit den Standardabschlussverfahren fortfahren.

Upgrade-Ressourcen (falls zutreffend): Im folgenden offiziellen Cisco Dokument finden Sie detaillierte Anweisungen zum Durchführen des Upgrades für Cisco Cloud-Pro und Cisco On-Prem: Cisco SD-WAN-Upgrade-Leitfaden

Ein allgemeiner Überblick über den Upgrade-Prozess umfasst:

1. Laden Sie die entsprechenden Software-Images in Ihr Manager (vManage) Repository hoch.
2. Die Controller werden nacheinander aktualisiert, beginnend mit Manager (vManage), gefolgt von Validator (vBond) und Controller (vSmart).
3. Aktivieren der neuen Softwareversionen und Überprüfen der Systemfunktionalität.

Wir werden Ihren Fall weiterhin überwachen. Wenn wir innerhalb von 10 Geschäftstagen nach Bereitstellung aller Ergebnisse basierend auf den Dateien, die wir von Ihnen erhalten haben, keine Rückmeldung erhalten, gehen wir davon aus, dass keine weitere Unterstützung erforderlich ist, und fahren Sie mit den normalen TAC-Verfahren zum Schließen von Fällen fort. Wenn Sie Hilfe benötigen, teilen Sie uns dies bitte mit.

Mit freundlichen Grüßen

ⓘ Ersetzen Sie alle **[Platzhalter in Klammern]** vor dem Senden.

✉ Outlook öffnen (nur Betreff)

⬇ EML-Vorlage herunterladen

Sherlock 3 - Erinnerung - Admin-Tech-Dateien fehlen

Anwendungsfall

Automatische Nachverfolgung, wenn die übermittelten Admin-Tech-Dateien nicht mit der Anzahl der SD-WAN-Steuerungskomponenten in den Protokollen übereinstimmen

Betreff

Erinnerung: Admin-Tech-Dateien für CVE-2026-20182-Analyse fehlen

Nachricht

Sehr geehrter Kunde,

Es fehlen immer noch Admin-Technik aus Ihren SD-WAN-Steuerungskomponenten, sodass unser System keine Indicators of Compromise aus den Admin-Tech-Protokollen auswerten kann. Um mit der CVE-2026-20182-Analyse zu beginnen, müssen wir Admin-Tech-Dateien von ALLEN Controllern (vSmarts), Validatoren (vBonds) und Managern (vManage) erhalten, einschließlich aller Manager (vManage)-Knoten, sofern diese geclustert sind.

Weitere Schritte:

Laden Sie die verbleibenden Admin-Tech-Dateien so bald wie möglich hoch.

Mit freundlichen Grüßen

In Outlook öffnen

ⓘ Ersetzen Sie alle **[Platzhalter in Klammern]** vor dem Senden.

✉ Outlook öffnen (mit Text)

⬇ EML-Vorlage herunterladen

TAC 1 - Untersuchung - weitere Überprüfung erforderlich (IoC-Verdacht)

Anwendungsfall

Wird vom TAC-Techniker gesendet, sobald die Automatisierung Protokolle gefunden hat, die auf eine mögliche Kompromittierung und eine Untersuchung durch einen Mitarbeiter hinweisen.

Betreff

SR-Nr.: Weitere Untersuchungen erforderlich

Nachricht

Sehr geehrter Kunde,

Mein Name ist {your_name}, und ich habe Ihren Fall akzeptiert. Vielen Dank für Ihre fortgesetzte Zusammenarbeit mit dem Cisco Technical Assistance Center (TAC).

Nach einer vorläufigen Analyse der Admin-Tech-Dateien, die Sie aus **Ihren SD-WAN-Steuerungskomponenten** bereitgestellt haben, haben wir festgestellt, dass eine weitere TAC-Untersuchung erforderlich ist, um unsere Analyse abzuschließen. Um eine gründliche und genaue Lösung zu gewährleisten, werde ich bei den nächsten Schritten eng mit Ihnen zusammenarbeiten.

Seien Sie versichert, dass wir Sie bei den nächsten Schritten unterstützen und Ihnen klare Leitlinien an die Hand geben werden, um die Situation effektiv anzugehen.

Geben Sie Ihrer Upgrade-Planung und -Durchführung Priorität, da dies der wichtigste Schritt zur Minderung dieses Risikos ist. Wenn Sie dieses Upgrade noch nicht geplant haben, führen Sie es bitte sofort durch.

Wenn Sie Fragen haben oder Hilfe benötigen, wenden Sie sich bitte an Ihren TAC-Techniker.

Vielen Dank für Ihre Aufmerksamkeit und Zusammenarbeit.

Mit freundlichen Grüßen

In Outlook öffnen

① Ersetzen Sie alle **[Platzhalter in Klammern]** vor dem Senden.

✉ Outlook öffnen (mit Text)

📎 EML-Vorlage herunterladen

TAC 2 - Ergebnis - Keine IoCs gefunden (vom Techniker bestätigt)

Anwendungsfall

Wird vom TAC-Techniker gesendet, sobald die Automatisierung keine Anzeichen für eine Kompromittierung gefunden hat und der Techniker das Ergebnis bestätigt hat.

Betreff

Update: TAC-Überprüfung abgeschlossen - Keine IoCs für CVE-2026-20182 gefunden - Ticket [SR #]

Nachricht

Hallo [Kundenname],

Ich bin der Cisco TAC-Techniker, der Ihrem Ticket zugewiesen ist [SR-Nummer].

Nach einer ersten Überprüfung der Admin-Tech-Dateien, die Sie von Ihren SD-WAN-Steuerungskomponenten bereitgestellt haben, konnten wir keine Protokolleinträge finden, die mit den in den Cisco SD-WAN-Sicherheitsempfehlungen beschriebenen Indicators of Compromise übereinstimmen:

- **Sicherheitslücke bei Cisco Catalyst SD-WAN-Controller-Authentifizierung umgangen [1]**
- **Sicherheitslücken im Cisco Catalyst SD-WAN Manager [2]**

Sie sollten jedoch alle Komponenten Ihrer SD-WAN-Steuerung auf <Version einfügen> aktualisieren. So setzen Sie das Upgrade fort:

- **Starten Sie Ihr Catalyst SD-WAN-Upgrade [3]**
- **Cisco SD-WAN-Upgrade-Leitfaden[4]**

Bitte beachten Sie, dass Cisco aufgrund der Dynamik der IP-Adressierung im Internet und unserer fehlenden Kenntnis der erwarteten IP-Adressen von Edge-Geräten im Netzwerk eines Kunden keine Protokolle von Edge-Geräten auswerten kann. Kunden werden aufgefordert, zur manuellen Durchführung dieses Schritts die in der Sicherheitsempfehlung für die Umgehung von Schwachstellen angegebenen Leitfäden zur Peering-Ereignisvalidierung zu befolgen. Es wird außerdem empfohlen, die zusätzlichen Schritte zur Erkennung im Zusammenhang mit der Überprüfung von Peering-Ereignissen durchzuführen, wie im Sicherheitsratgeber für CVE-2026-20182 beschrieben.

Links

[1] Sicherheitslücke bei Authentifizierung des Cisco Catalyst SD-WAN-Controllers umgangen -

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

[2] Sicherheitslücken beim Cisco Catalyst SD-WAN Manager:

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

[3] Starten Sie Ihr 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-Leitfaden: <https://www.cisco.com/c/en/us/support/docs/wan/dpt/220424-upgrade-sd-wan-controllers-with-the-use.html>

Mit freundlichen Grüßen

In Outlook öffnen

① Ersetzen Sie alle **[Platzhalter in Klammern]** vor dem Senden.

✉ Outlook öffnen (nur Betreff)

⬇ EML-Vorlage herunterladen

TAC 3 - Validierung - IP-Eigentumsrechte an Overlay bestätigen

Anwendungsfall

Wird vom TAC-Techniker gesendet, um den Kunden zu fragen, ob spezifische IP-Adressen, die während der Protokollanalyse angezeigt werden, Teil seiner SD-WAN-Overlay-Infrastruktur sind oder waren.

Betreff

[SR-Nr.] - Validierung der IP-Adresse erforderlich

Nachricht

Sehr geehrte/r Frau/Herr [Kundenname],

Mein Name ist [Ihr Name], und ich bin der Cisco TAC-Techniker, der Ihrem Ticket zugewiesen ist.

Im Rahmen unserer laufenden Analyse der Admin-Tech-Dateien, die Sie von Ihren SD-WAN-Steuerungskomponenten bereitgestellt haben, benötigen wir Ihre Unterstützung bei der Überprüfung, ob die folgenden IP-Adressen Teil Ihrer SD-WAN-Overlay-Infrastruktur sind oder waren:

IP-Adresse(n):

- [IP-Adresse 1]
- [IP-Adresse 2]

Bestätigen Sie Folgendes, um uns bei der Bewertung zu unterstützen:

1. Ist diese IP-Adresse derzeit mit einer Komponente Ihres SD-WAN-Overlays (z. B. vManage, vSmart, vBond oder Edge-Gerät) verknüpft?
2. Wurde diese IP-Adresse zuvor von einer SD-WAN-Steuerungskomponente verwendet, die möglicherweise außer

Betrieb genommen wurde oder deren IP geändert wurde?

3. Ist diese IP mit einem Disaster Recovery-Standort (DR) oder einer anderen Infrastruktur in Verbindung mit Ihrer SD-WAN-Bereitstellung verbunden?

Ihre umgehende Antwort ermöglicht es uns, unsere Analyse fortzusetzen und Ihnen die entsprechenden nächsten Schritte bereitzustellen.

Wenn Sie Fragen haben, zögern Sie bitte nicht, sich an uns zu wenden.

Mit freundlichen Grüßen

In Outlook öffnen

❗ Ersetzen Sie alle [Platzhalter in Klammern] vor dem Senden.

✉ Outlook öffnen (mit Text)

📎 EML-Vorlage herunterladen

TAC 4 - Ergebnis - Falsch positiv geklärt

Anwendungsfall

Wird vom TAC-Techniker nach einer manuellen Überprüfung versendet, wird festgestellt, dass das ursprüngliche IoC, das durch automatisierte Scans gekennzeichnet wurde, falsch positiv war.

Betreff

Update: Technische Bewertung von CVE-2026-20182 - Case [Case Number]

Nachricht

Sehr geehrter Kunde,

Vielen Dank für Ihre Geduld, während unser Technikerteam eine manuelle Überprüfung der Admin-Tech-Dateien durchgeführt hat, die Sie von Ihren SD-WAN-Steuerungskomponenten bereitgestellt haben.

Nach einer gründlichen Untersuchung haben wir festgestellt, dass der ursprüngliche Indikator für Kompromittierung (IoC), der durch unseren automatisierten Scanvorgang gekennzeichnet wurde, falsch positiv war, d. h., unsere Einschätzung ist, dass die IoCs ungültig sind.

Wichtig: Beachten Sie, dass die mit [CVE-2026-20182](#)^[1] verbundene Schwachstelle ein Software-Upgrade erfordert, um die Sicherheit und Integrität Ihrer SD-WAN-Fabric langfristig zu gewährleisten.

Wenn Sie das Upgrade noch nicht abgeschlossen haben: Priorisieren Sie so bald wie möglich das vollständige Upgrade Ihrer SD-WAN-Steuerungskomponenten. Das Upgrade ist die einzige Möglichkeit, diese Schwachstelle zu beheben. Ausführliche Anweisungen finden Sie im [Cisco SD-WAN-Upgrade-Leitfaden](#) [2].

Wenn Sie das Upgrade bereits abgeschlossen haben: Da wir diese Feststellung als falsch bestätigt haben und Sie die Software-Korrektur bereits durchgeführt haben, sind keine weiteren Maßnahmen erforderlich. Sie können diesen Fall als gelöst betrachten und mit den Standardverfahren zur Schließung fortfahren.

Wir freuen uns, dass Sie die Sicherheit Ihrer Infrastruktur mit größter Sorgfalt priorisieren. Wenn Sie weitere Fragen haben oder zusätzliche Unterstützung benötigen, wenden Sie sich bitte an uns.

Mit freundlichen Grüßen

Cisco Technical Assistance Center (TAC)

Links:

[1] [Offizielles Sicherheitshinweis](#)

[2] [Cisco SD-WAN-Upgrade-Leitfaden](#)

In Outlook öffnen

📘 Ersetzen Sie alle **[Platzhalter in Klammern]** vor dem Senden.

📧 Outlook öffnen (nur Betreff)

📎 EML-Vorlage herunterladen

TAC 5 - Kritisch - IoC identifiziert, Zeitplan Überprüfung Anruf

Anwendungsfall

Wird vom TAC-Techniker versendet, wenn potenzielle Indicators of Compromise bestätigt wurden und ein dringender Kundenanruf erforderlich ist, um die Ergebnisse und die nächsten Schritte zu besprechen.

Betreff

DRINGEND: Analyseergebnisse für CVE-2026-20182 - Indicator of Compromise identifiziert

Nachricht

Sehr geehrter Kunde,

Wir danken Ihnen für Ihre Geduld, während wir die für Ihre SD-WAN-Steuerungskomponenten bereitgestellten Admin-Tech-Dateien analysiert haben.

Nach unserer technischen Überprüfung haben wir potenzielle Indicators of Compromise (IoCs) im Zusammenhang mit CVE-2026-20182 identifiziert.

Ansichts der Art dieser Ergebnisse ist es von entscheidender Bedeutung, dass wir die technischen Details und die empfohlenen nächsten Schritte so bald wie möglich erörtern. Gerne vereinbaren wir mit Ihrem Team einen Termin für ein Gespräch, um die Ergebnisse genauer zu besprechen und die geeignete Behebung zu besprechen.

Weitere Schritte:

- **Ein Meeting ansetzen:** Teilen Sie uns bitte mit, ob Sie innerhalb der nächsten [z. B. 4-8 Stunden] einen kurzen Anruf erhalten, um die Ergebnisse zu besprechen.
- **SDWAN-Steuerungskomponenten aktualisieren:** Aktualisieren Sie Ihren SDWAN Manager, Controller und Validator so bald wie möglich auf eine feste Version.

Unser vorrangiges Ziel ist es, Sie bei der Sicherung Ihrer Umgebung und der Minderung potenzieller Risiken zu unterstützen. Wir freuen uns, dass Sie sich umgehend mit dieser Angelegenheit befassen und uns mit Ihnen abstimmen werden.

Mit freundlichen Grüßen

In Outlook öffnen

📘 Ersetzen Sie alle **[Platzhalter in Klammern]** vor dem Senden.

📧 Outlook öffnen (mit Text)

📎 EML-Vorlage herunterladen

TAC 6 - Ergebnis - Doppeltes IoC (Schließen und Umleiten)

Anwendungsfall

Wird vom TAC-Techniker gesendet, wenn die IoC-Analyse die Ergebnisse bestätigt, die mit einer früheren Serviceticket für denselben Kunden bzw. dieselbe Umgebung übereinstimmen. Der aktuelle Fall ist abgeschlossen, und der Kunde wird an den ursprünglichen Serviceticket weitergeleitet, für das bereits eine Anleitung zur Problembeseitigung bereitgestellt wurde.

Betreff

Update: Technische Überprüfung für CVE-2026-20182 - Case [SR-Nr.] (Doppeltes IoC bestätigt)

Nachricht

Sehr geehrter Kunde,

Wir danken Ihnen für Ihre Geduld, während wir die für Ihre SD-WAN-Steuerungskomponenten bereitgestellten Admin-Tech-Dateien analysiert haben. Wir haben festgestellt, dass die durch den Scanvorgang gekennzeichneten ersten Indicators of Compromise (IoC) mit den bereits in **[Original SR #]** gemeldeten Indicators of Compromise übereinstimmen. Wie bereits erwähnt, empfehlen wir dringend ein Upgrade und die Durchführung eines der beiden im [TAC-Sanierungsleitfaden](#) ^[2] beschriebenen Sanierungspfade, um Ihre Umgebung so schnell wie möglich zu schützen. Ausführliche Informationen finden Sie in der [offiziellen Sicherheitsempfehlung für CVE-2026-20182](#) ^[1].

Ich schließe das Verfahren jetzt ab. Verwenden Sie **[Original SR #]**, um weitere Unterstützung oder technischen Support für Ihr Upgrade oder Ihre Problembehebung anzufordern.

Mit freundlichen Grüßen

[Ihr Name]

Links:

[1] [Offizielles Sicherheitshinweis](#)

[2] [TAC-Sanierungsleitfaden](#)

In Outlook öffnen

① Ersetzen Sie alle **[Platzhalter in Klammern]** vor dem Senden.

✉ Outlook öffnen (mit Text)

📎 EML-Vorlage herunterladen

TAC 7 - Problembehebung - Follow-up-Optionen (nach Anruf)

Anwendungsfall

Wird nach dem IoC-Überprüfungsaufwurf gesendet, um die besprochenen Problembehebungspfade zusammenzufassen. Der Kunde wählt Option A (erneute Bereitstellung mit fortlaufendem Neustart), Option B (erneute Bereitstellung mit fester Umstellung) oder Option C (vollständige Systemwiederherstellung).

Betreff

Weiteres Vorgehen: Sanierungsoptionen für CVE-2026-20182

Nachricht

Sehr geehrter Kunde,

Vielen Dank für die Zeit, die Sie sich für die Besprechung der Ergebnisse unserer aktuellen Analyse genommen haben. Wie bereits erwähnt, empfehlen wir zur Sicherung Ihrer Umgebung die folgenden Optionen zur Problembehebung.

Option A: Neubereitstellung mit rollendem Neustart. Zur Gewährleistung der Betriebskontinuität müssen Netzwerkausfälle vermieden werden. Gleichzeitig bleibt das Risiko bestehen, dass die Bedrohung während des Übergangsprozesses anhält.

Beschreibung: Umfassende Controller-Neubereitstellung sowie SSH-Schlüssel- und Zertifikatsrotation. Bestehende Controller-Komponenten werden während der Migration über vManage zur Bereitstellung der neuen Fabric verbunden und nach der Migration des Geräts entfernt.

Option B: Umverteilung mit harter Umstellung. Bietet ein höheres Maß an Sicherheit. Da neue Controller nie mit alten Controllern verbunden werden, gibt es eine vollständige Isolierung. Dies hat Auswirkungen auf den gesamten Netzwerkbetrieb, da alle Geräte die Verbindung wiederherstellen und Routen-/Verbindungsinformationen austauschen müssen. Die Ausfallzeit hängt von der Anzahl der Standorte, der ausgetauschten Präfixe usw. ab.

Beschreibung: Umfassende Controller-Neubereitstellung plus SSH-Schlüssel- und Zertifikatsrotation, aber die alten Controller-Komponenten werden während der Neubereitstellung von der neuen Fabric isoliert.

Option C: Vollständige Systemwiederherstellung Bietet ein Höchstmaß an Sicherheit durch die Erstellung einer sauberen Baseline. Dies ist jedoch der komplexeste Ansatz und birgt ein höheres Risiko konfigurationsbedingter Instabilität während der Wiederherstellung. Dies ist eine langwierige Option und erfordert Fachwissen beim Neuaufbau der Vorlagen- und Richtliniendatenbanken.

Weitere Schritte:

- Besprechen Sie diese Optionen bitte intern, und teilen Sie uns mit, welchen Weg Sie einschlagen möchten. Sobald Sie sich entschieden haben, können wir Ihnen weitere Anleitungen oder technischen Support zur Verfügung stellen, um Sie während der Ausführungsphase zu unterstützen.

Wir sind hier, um Sie während dieses Prozesses zu unterstützen. Bitte teilen Sie uns mit, wenn Sie Fragen zu diesen Optionen haben.

Mit freundlichen Grüßen

Cisco Technical Assistance Center (TAC)

HINWEIS: Option 1 war das Upgrade. Das Szenario, in dem davon ausgegangen wird, dass dieses Upgrade bereits durchgeführt wurde.

In Outlook öffnen

① Verwenden Sie die .eml-Download unten. Ersetzen Sie alle **[Platzhalter in Klammern]** vor dem Senden.

✉ Outlook öffnen (nur Betreff)

↓ EML-Vorlage herunterladen

TAC 8 - Problembehebung - Aktualisierte Optionen für kompromittierte Strukturen (Option 2)

Anwendungsfall

Kunden zu benachrichtigen, deren SD-WAN-Fabrics gefährdet waren und zuvor Option 2 verfolgten und deren Fabrics weiterhin dem Risiko des Fortbestands von Angreifern ausgesetzt sind. Kunden, die ihre kompromittierte Fabric neu erstellt haben (und sich nicht auf ein Backup/eine vorhandene Konfigurationsdatenbank verlassen haben), werden nicht als gefährdet eingestuft und erhalten diese Mitteilung nicht. Diese Mitteilung wird von TBD versendet.

Betreff

Dringende Maßnahmen erforderlich: Beseitigung kritischer Schwachstellen in der SD-WAN-Infrastruktur

Nachricht

Sehr geehrter Kunde,

Wir stellen ein wichtiges Update für die Sanierung Ihrer SD-WAN-Fabric bereit, wie in [SR#] und den zuvor übermittelten Sicherheitsankündigungen beschrieben. Diese Aktualisierung bezieht sich speziell auf Fabrics, in denen die übermittelten Protokolle Anzeichen für Indicators of Compromise (IOCs) aufwiesen.

Während Sie sich bereits für einen Sanierungsplan basierend auf Option 2 entschieden haben, der ein Software-Upgrade, die Neubereitstellung von Controllern und die SSH-Schlüsselrotation beinhaltet, hat sich unsere Analyse der Bedrohungslandschaft weiter entwickelt. Neue technische Erkenntnisse über die Ausnutzung dieser Schwachstellen zeigen, dass dringend zusätzliche Maßnahmen ergriffen werden müssen, um das Risiko der Persistenz zu verringern und die Integrität der Zertifikatskette zu gewährleisten.

MASSNAHME ERFORDERLICH:

Wir haben die empfohlenen Wiederherstellungsstrategien aktualisiert, um einen umfassenderen Schutz durch die zusätzliche Rotation von Stammzertifikaten bereitzustellen.

Bitte beachten Sie, dass die Behebung zusätzliche Wartungsarbeiten erfordert, die geplante Netzwerkausfälle einschließen können.

Da Sicherheit und Integrität Ihres Netzwerks höchste Priorität haben, haben wir drei Optionen für die Problembehebung entwickelt. Jede der folgenden Optionen bietet ein ausgewogenes Verhältnis zwischen betrieblichen Auswirkungen und Sicherheitsgarantien. Da Ihr interner Risikostatus einzigartig ist, kann Cisco keinen bestimmten Pfad empfehlen.

Option A: Neubereitstellung mit rollendem Neustart. Zur Gewährleistung der Betriebskontinuität müssen Netzwerkausfälle vermieden werden. Gleichzeitig bleibt das Risiko bestehen, dass die Bedrohung während des Übergangsprozesses anhält.

Beschreibung: Umfassende Controller-Neubereitstellung sowie SSH-Schlüssel- und Zertifikatsrotation. Bestehende Controller-Komponenten werden während der Migration über vManage zur Bereitstellung der neuen Fabric verbunden

und nach der Migration des Geräts entfernt.

Option B: Umverteilung mit harter Umstellung. Bietet ein höheres Maß an Sicherheit. Da neue Controller nie mit alten Controllern verbunden werden, gibt es eine vollständige Isolierung. Dies hat Auswirkungen auf den gesamten Netzwerkbetrieb, da alle Geräte die Verbindung wiederherstellen und Routen-/Verbindungsinformationen austauschen müssen. Die Ausfallzeit hängt von der Anzahl der Standorte, der ausgetauschten Präfixe usw. ab.

Beschreibung: Umfassende Controller-Neubereitstellung plus SSH-Schlüssel- und Zertifikatrotation, aber die alten Controller-Komponenten werden während der Neubereitstellung von der neuen Fabric isoliert.

Option C: Vollständige Systemwiederherstellung Bietet ein Höchstmaß an Sicherheit durch die Erstellung einer sauberen Baseline. Dies ist jedoch der komplexeste Ansatz und birgt ein höheres Risiko konfigurationsbedingter Instabilität während der Wiederherstellung. Dies ist eine langwierige Option und erfordert Fachwissen beim Neuaufbau der Vorlagen- und Richtliniendatenbanken.

Wenn Ihr Team diese Optionen geprüft und den Ansatz ermittelt hat, der am besten zu Ihren Risikomanagementstandards passt, teilen Sie uns dies bitte mit, indem Sie auf diese Nachricht antworten. Nach Erhalt Ihrer Auswahl koordinieren wir das Wartungsfenster und beginnen die notwendigen technischen Vorbereitungen für die Ausführung.

Wir freuen uns, dass Sie sich weiterhin auf die Wartung einer sicheren Netzwerkinfrastruktur konzentrieren. Wenn Sie weitere technische Informationen benötigen, senden Sie uns bitte ein Serviceticket (SR) beim Technical Assistance Center (TAC).

Mit freundlichen Grüßen
Cisco

In Outlook öffnen

① Verwenden Sie die .eml-Download unten. Ersetzen Sie alle **[Platzhalter in Klammern]** vor dem Senden.

✉ Outlook öffnen (nur Betreff)

↓ EML-Vorlage herunterladen

TAC 17 - Reversed Finding - früher kein IoC, jetzt IoC identifiziert (CVE-2026-20182)

Anwendungsfall

Wird an Kunden gesendet, die **zuvor darüber informiert** wurden, dass **keine Indicators of Compromise (IoCs)** gefunden wurden, für die jedoch seitdem eine **spätere interne Überprüfung** von Admin-Tech-Protokollen **IoCs** im Zusammenhang mit CVE-2026-20182 **identifiziert** hat. Überarbeitet die Ergebnisse und bietet die drei Sanierungsoptionen (Option A, B oder C).

Betreff

Wichtiges Update: Überarbeitete IoC-Bewertung für CVE-2026-20182 - Indicators of Compromise jetzt identifiziert - SR [SR#]

Nachricht

Sehr geehrter Kunde,

vielen Dank für Ihre fortgesetzte Zusammenarbeit mit dem Cisco Technical Assistance Center (TAC) in Bezug auf CVE-2026-20182 unter der Serviceanfrage [SR#].

In unserer vorherigen Korrespondenz haben wir darauf hingewiesen, dass unsere Analyse der Admin-Tech-Dateien, die von Ihren SD-WAN-Steuerungskomponenten bereitgestellt werden, keine Indicators of Compromise (IoCs) im Zusammenhang mit dieser Ankündigung identifiziert. Im Rahmen unseres fortwährenden Engagements für Ihre Sicherheit haben wir seither eine routinemäßige interne Überprüfung zusätzlicher administrativer Protokolldaten im Zusammenhang mit der Fabric Ihres Unternehmens durchgeführt.

Bei dieser anschließenden Überprüfung wurden Indicators of Compromise (IoCs) identifiziert, die bei der ersten Bewertung nicht aufgedeckt wurden. Wir arbeiten nun gemeinsam mit Ihnen an der Auswertung dieser Ergebnisse. Diese IoCs weisen auf potenziell verdächtige Aktivitäten in der Fabric Ihres Unternehmens hin, die Abhilfemaßnahmen rechtfertigen.

Wir erkennen an, dass dies das Ergebnis, das Ihnen zuvor mitgeteilt wurde, überarbeitet, und wir möchten sicherstellen, dass Sie ein klares und genaues Bild von Ihrer Umgebung haben, sodass die entsprechende Sanierung vorgenommen werden kann.

MASSNAHME ERFORDERLICH:

Bitte beachten Sie, dass die Behebung zusätzliche Wartungsarbeiten erfordert, die geplante Netzerkausfälle einschließen können.

Da Sicherheit und Integrität Ihres Netzwerks höchste Priorität haben, haben wir drei Optionen für die Problembehebung entwickelt. Jede der folgenden Optionen bietet ein ausgewogenes Verhältnis zwischen betrieblichen Auswirkungen und Sicherheitsgarantien. Da Ihr interner Risikostatus einzigartig ist, kann Cisco keinen bestimmten Pfad empfehlen.

Option A: Neubereitstellung mit rollendem Neustart. Zur Gewährleistung der Betriebskontinuität müssen Netzerkausfälle vermieden werden. Gleichzeitig bleibt das Risiko bestehen, dass die Bedrohung während des Übergangsprozesses anhält.

Beschreibung: Umfassende Controller-Neubereitstellung sowie SSH-Schlüssel- und Zertifikatsrotation. Bestehende Controller-Komponenten werden während der Migration über vManage zur Bereitstellung der neuen Fabric verbunden und nach der Migration des Geräts entfernt.

Option B: Umverteilung mit harter Umstellung. Bietet ein höheres Maß an Sicherheit. Da neue Controller nie mit alten

Controllern verbunden werden, gibt es eine vollständige Isolierung. Dies hat Auswirkungen auf den gesamten Netzwerkbetrieb, da alle Geräte die Verbindung wiederherstellen und Routen-/Verbindungsinformationen austauschen müssen. Die Ausfallzeit hängt von der Anzahl der Standorte, der ausgetauschten Präfixe usw. ab.

Beschreibung: Umfassende Controller-Neubereitstellung plus SSH-Schlüssel- und Zertifikatrotation, aber die alten Controller-Komponenten werden während der Neubereitstellung von der neuen Fabric isoliert.

Option C: Vollständige Systemwiederherstellung Bietet ein Höchstmaß an Sicherheit durch die Erstellung einer sauberen Baseline. Dies ist jedoch der komplexeste Ansatz und birgt ein höheres Risiko konfigurationsbedingter Instabilität während der Wiederherstellung. Dies ist eine langwierige Option und erfordert Fachwissen beim Neuerstellen der Vorlagen- und Richtliniendatenbanken.

Wenn Ihr Team diese Optionen geprüft und den Ansatz ermittelt hat, der am besten zu Ihren Risikomanagementstandards passt, teilen Sie uns dies bitte mit, indem Sie auf diese Nachricht antworten. Nach Erhalt Ihrer Auswahl koordinieren wir das Wartungsfenster und beginnen die notwendigen technischen Vorbereitungen für die Ausführung.

Wir freuen uns, dass Sie sich weiterhin auf die Wartung einer sicheren Netzwerkinfrastruktur konzentrieren. Wenn Sie weitere technische Informationen benötigen, senden Sie uns bitte eine Antwort auf diese E-Mail, oder senden Sie eine bestehende Serviceanfrage (Service Request, SR) an unser Technical Assistance Center (TAC).

Mit freundlichen Grüßen
Cisco

In Outlook öffnen

① Verwenden Sie die .eml-Download unten. Ersetzen Sie alle **[Platzhalter in Klammern]** vor dem Senden.

✉ Outlook öffnen (nur Betreff)

↓ EML-Vorlage herunterladen

CloudOps 1 - Proaktiv - IoC beim Cloud-Scan erkannt, Admin-Tech zur Validierung erforderlich

Anwendungsfall

Proaktiv gesendet, wenn bei einem Sicherheitsscan einer in der Cloud gehosteten SD-WAN-Fabric durch Cisco CloudOps potenzielle Indicators of Compromise (IoCs) aufgetaucht sind. Im Namen des Kunden wird ein Serviceticket geöffnet, und der Kunde wird gebeten, Admin-Tech-Dateien anzuhängen, damit die Ergebnisse durch vollständige Protokollanalyse validiert werden können.

Betreff

Maßnahme erforderlich: Admin-Tech-Dateien zur Überprüfung der Ergebnisse von Sicherheitsprüfungen - SR [SR#]

Nachricht

Sehr geehrter Kunde,

Im Rahmen unserer fortlaufenden Bemühungen, die Integrität der Cisco Angebote zu sichern und zu überwachen, hat Cisco kürzlich eine Sicherheitsprüfung ausgewählter Cloud-gehosteter SD-WAN-Fabrics durchgeführt. Diese Aktion wurde als Reaktion auf ein gemeldetes Sicherheitsproblem durchgeführt. Der Scan hat potenziell verdächtige Aktivitäten in der Fabric Ihres Unternehmens identifiziert, die eine weitere Überprüfung erfordern.

Wir bitten Sie, dieser in Ihrem Auftrag erstellten Serviceanfrage (Service Request, SR) Admin-Tech-Dateien hinzuzufügen, damit wir diese Feststellung validieren und unsere Untersuchung abschließen können.

Um eine vollständige Analyse zu ermöglichen, erfassen und laden Sie Admin-Tech-Dateien von allen SD-WAN-Steuerungskomponenten hoch. Wählen Sie beim Generieren dieser Dateien sowohl **"Protokolle"** als auch **"Tech"** aus:

- **vSmarts (Controller):** Sammeln Sie eine nach der anderen, nicht gleichzeitig.
- **vBonds (Prüfer):** Von allen Knoten sammeln.
- **Manager (vManage):** Sammeln Sie alle Knoten im Cluster (Active und Standby-DR).

Detaillierte, schrittweise Anleitungen zum Generieren und sicheren Senden Ihrer Admin-Tech-Dateien finden Sie in diesem Handbuch: [Cisco SD-WAN Admin-Tech Collection-Leitfaden](#)^[1].

Sobald die angeforderten Dateien bei uns eingegangen sind, wird unser Team sie analysieren, um festzustellen, ob die beobachtete Aktivität einen echten Indicator of Compromise darstellt, und Sie über die nächsten Schritte informieren.

Wir freuen uns, dass Sie sich weiterhin auf die Wartung einer sicheren Netzwerkinfrastruktur konzentrieren. Bitte teilen Sie uns mit, wenn Sie weitere technische Informationen benötigen, indem Sie auf diese Serviceanfrage (SR) antworten.

Mit freundlichen Grüßen

Cisco

Links:

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

In Outlook öffnen

① Verwenden Sie die .eml-Download unten. Ersetzen Sie alle **[Platzhalter in Klammern]** vor dem Senden.

✉ Outlook öffnen (nur Betreff)

↓ EML-Vorlage herunterladen

E-Mails für WAVE 2A für ZUVOR BETROFFENE Kunden, die die Optionen A, B ODER C noch nicht abgeschlossen haben (die

Optionen 1 und 2 müssen erneut durchgeführt werden)

TAC 9-Vorlage ohne IOC für PSIRT2a/wurde neu erstellt (**VORHER AUSGEFÜHRT**)

Anwendungsfall

Wird an Kunden gesendet, deren SD-WAN-Protokolle **keine Indicators of Compromise (IoCs)** im Zusammenhang mit dem PSIRT2a Advisory AND aufwiesen, die **zuvor** ihre Fabric **neu aufgebaut hatten**. Bietet aktualisierte Anleitungen für die Problembehebung mit drei Optionen (Option 2 für die Nachbereitung).

Betreff

Dringende Maßnahmen erforderlich: SD-WAN Infrastructure Critical Vulnerability Remediation - SR [SR#]

Nachricht

Sehr geehrter Kunde,

vielen Dank, dass Sie das Cisco Technical Assistance Center (TAC) bezüglich der aktuellen PSIRT-Empfehlungen für das SD-WAN unter der Serviceanfrage [SR#] kontaktiert haben.

Nach der Überprüfung der Protokolle und Informationen aus Ihrer SD-WAN-Fabric hat unsere Analyse keine Indicators of Compromise (IOCs) im Zusammenhang mit der Sicherheitslücke in SD-WAN vom 5. Juni 2026 identifiziert. Darüber hinaus haben wir festgestellt, dass Ihre Umgebung im Rahmen der mit früheren Warnmeldungen zusammenhängenden Maßnahmen zur Problembehebung bereits wiederhergestellt wurde.

Angesichts neu gewonnener Erkenntnisse möchten wir Sie über die empfohlenen Sanierungsleitfäden für SD-WAN-Strukturen informieren.

Wir stellen ein wichtiges Update für die Sanierung Ihrer SD-WAN-Fabric bereit, wie in [SR#] und den zuvor übermittelten Sicherheitsankündigungen beschrieben.

Während Sie sich bereits für einen Sanierungsplan basierend auf Option 2 entschieden haben, der ein Software-Upgrade, die Neubereitstellung von Controllern und die SSH-Schlüsselrotation beinhaltet, hat sich unsere Analyse der Bedrohungslandschaft weiter entwickelt. Neue technische Erkenntnisse über die Ausnutzung dieser Schwachstellen zeigen, dass dringend zusätzliche Maßnahmen ergriffen werden müssen, um das Risiko der Persistenz zu verringern und die Integrität der Zertifikatskette zu gewährleisten.

MASSNAHME ERFORDERLICH:

Wir haben die empfohlenen Wiederherstellungsstrategien aktualisiert, um einen umfassenderen Schutz durch die zusätzliche Rotation von Stammzertifikaten bereitzustellen.

Bitte beachten Sie, dass die Behebung zusätzliche Wartungsarbeiten erfordert, die geplante Netzwerkausfälle einschließen können. Da Sicherheit und Integrität Ihres Netzwerks höchste Priorität haben, haben wir drei Optionen für die Problembehebung entwickelt. Jede der folgenden Optionen bietet ein ausgewogenes Verhältnis zwischen betrieblichen Auswirkungen und Sicherheitsgarantien. Da Ihr interner Risikostatus einzigartig ist, kann Cisco keinen bestimmten Pfad empfehlen.

Option A: Neubereitstellung mit rollendem Neustart. Zur Gewährleistung der Betriebskontinuität müssen Netzwerkausfälle vermieden werden. Gleichzeitig bleibt das Risiko bestehen, dass die Bedrohung während des Übergangsprozesses anhält.

Beschreibung: Umfassende Controller-Neubereitstellung sowie SSH-Schlüssel- und Zertifikatsrotation. Bestehende Controller-Komponenten werden während der Migration über vManage zur Bereitstellung der neuen Fabric verbunden und nach der Migration des Geräts entfernt.

Option B: Umverteilung mit harter Umstellung. Bietet ein höheres Maß an Sicherheit. Da neue Controller nie mit alten Controllern verbunden werden, gibt es eine vollständige Isolierung. Dies hat Auswirkungen auf den gesamten Netzwerkbetrieb, da alle Geräte die Verbindung wiederherstellen und Routen-/Verbindungsinformationen austauschen müssen. Die Ausfallzeit hängt von der Anzahl der Standorte, der ausgetauschten Präfixe usw. ab.

Beschreibung: Umfassende Controller-Neubereitstellung plus SSH-Schlüssel- und Zertifikatsrotation, aber die alten Controller-Komponenten werden während der Neubereitstellung von der neuen Fabric isoliert.

Option C: Vollständige Systemwiederherstellung Bietet ein Höchstmaß an Sicherheit durch die Erstellung einer sauberen Baseline. Dies ist jedoch der komplexeste Ansatz und birgt ein höheres Risiko konfigurationsbedingter Instabilität während der Wiederherstellung. Dies ist eine langwierige Option und erfordert Fachwissen beim Neuerstellen der Vorlagen- und Richtliniendatenbanken.

Wenn Ihr Team diese Optionen geprüft und den Ansatz ermittelt hat, der am besten zu Ihren Risikomanagementstandards passt, teilen Sie uns dies bitte mit, indem Sie auf diese Nachricht antworten. Nach Erhalt Ihrer Auswahl koordinieren wir das Wartungsfenster und beginnen die notwendigen technischen Vorbereitungen für die Ausführung.

Wir freuen uns, dass Sie sich weiterhin auf die Wartung einer sicheren Netzwerkinfrastruktur konzentrieren. Bitte teilen Sie uns mit, wenn Sie weitere technische Informationen benötigen, indem Sie auf diese E-Mail antworten oder die bestehende Serviceanfrage stellen.

Mit freundlichen Grüßen
Cisco

In Outlook öffnen

① Verwenden Sie die .eml-Download unten. Ersetzen Sie alle **[Platzhalter in Klammern]** vor dem Senden.

✉ Outlook öffnen (nur Betreff)

📎 EML-Vorlage herunterladen

TAC 10-Vorlage für yes IOC für PSIRT2a/they did rebuild (**PREVIOUSLY IMPACTED**)

Anwendungsfall

Wird an Kunden gesendet, deren SD-WAN-Protokolle **Indicators of Compromise (IoCs)** im Zusammenhang mit dem PSIRT2a Advisory UND zeigten, die **zuvor** ihre Fabric **neu aufgebaut hatten**. Bietet aktualisierte Anleitungen für die Problembehebung mit drei Optionen (Option 2 für die Nachbereitung).

Betreff

Dringende Maßnahmen erforderlich: SD-WAN Infrastructure Critical Vulnerability Remediation - SR [SR#]

Nachricht

Sehr geehrter Kunde,

vielen Dank, dass Sie das Cisco Technical Assistance Center (TAC) bezüglich der aktuellen PSIRT-Empfehlungen für das SD-WAN unter der Serviceanfrage [SR#] kontaktiert haben.

Nach der Analyse der Protokolle aus Ihrer SD-WAN-Fabric hat unser Team Indicators of Compromise (IOCs) identifiziert, die mit der Sicherheitslücke im SD-WAN vom 5. Juni 2026 in Verbindung stehen. Wir wissen auch, dass Ihre Umgebung im Rahmen von Sanierungsmaßnahmen, die mit früheren Empfehlungen in Zusammenhang stehen, zuvor einer Wiederherstellung unterzogen wurde.

Wir stellen ein wichtiges Update für die Sanierung Ihrer SD-WAN-Fabric bereit, wie in [SR#] und den zuvor übermittelten Sicherheitsankündigungen beschrieben. Diese Aktualisierung bezieht sich speziell auf Fabrics, in denen die übermittelten Protokolle Anzeichen für Indicators of Compromise (IOCs) aufwiesen.

Während Sie sich bereits für einen Sanierungsplan basierend auf Option 2 entschieden haben, der ein Software-Upgrade, die Neubereitstellung von Controllern und die SSH-Schlüsselrotation beinhaltet, hat sich unsere Analyse der Bedrohungslandschaft weiter entwickelt. Neue technische Erkenntnisse über die Ausnutzung dieser Schwachstellen zeigen, dass dringend zusätzliche Maßnahmen ergriffen werden müssen, um das Risiko der Persistenz zu verringern und die Integrität der Zertifikatskette zu gewährleisten.

MASSNAHME ERFORDERLICH:

Wir haben die empfohlenen Wiederherstellungsstrategien aktualisiert, um einen umfassenderen Schutz durch die zusätzliche Rotation von Stammzertifikaten bereitzustellen.

Bitte beachten Sie, dass die Behebung zusätzliche Wartungsarbeiten erfordert, die geplante Netzwerkausfälle

einschließen können. Da Sicherheit und Integrität Ihres Netzwerks höchste Priorität haben, haben wir drei Optionen für die Problembeseitigung entwickelt. Jede der folgenden Optionen bietet ein ausgewogenes Verhältnis zwischen betrieblichen Auswirkungen und Sicherheitsgarantien. Da Ihr interner Risikostatus einzigartig ist, kann Cisco keinen bestimmten Pfad empfehlen.

Option A: Neubereitstellung mit rollendem Neustart. Zur Gewährleistung der Betriebskontinuität müssen Netzerkämpfe vermieden werden. Gleichzeitig bleibt das Risiko bestehen, dass die Bedrohung während des Übergangsprozesses anhält.

Beschreibung: Umfassende Controller-Neubereitstellung sowie SSH-Schlüssel- und Zertifikatsrotation. Bestehende Controller-Komponenten werden während der Migration über vManage zur Bereitstellung der neuen Fabric verbunden und nach der Migration des Geräts entfernt.

Option B: Umverteilung mit harter Umstellung. Bietet ein höheres Maß an Sicherheit. Da neue Controller nie mit alten Controllern verbunden werden, gibt es eine vollständige Isolierung. Dies hat Auswirkungen auf den gesamten Netzbetrieb, da alle Geräte die Verbindung wiederherstellen und Routen-/Verbindungsinformationen austauschen müssen. Die Ausfallzeit hängt von der Anzahl der Standorte, der ausgetauschten Präfixe usw. ab.

Beschreibung: Umfassende Controller-Neubereitstellung plus SSH-Schlüssel- und Zertifikatsrotation, aber die alten Controller-Komponenten werden während der Neubereitstellung von der neuen Fabric isoliert.

Option C: Vollständige Systemwiederherstellung Bietet ein Höchstmaß an Sicherheit durch die Erstellung einer sauberen Baseline. Dies ist jedoch der komplexeste Ansatz und birgt ein höheres Risiko konfigurationsbedingter Instabilität während der Wiederherstellung. Dies ist eine langwierige Option und erfordert Fachwissen beim Neuerstellen der Vorlagen- und Richtliniendatenbanken.

Wenn Ihr Team diese Optionen geprüft und den Ansatz ermittelt hat, der am besten zu Ihren Risikomanagementstandards passt, teilen Sie uns dies bitte mit, indem Sie auf diese Nachricht antworten. Nach Erhalt Ihrer Auswahl koordinieren wir das Wartungsfenster und beginnen die notwendigen technischen Vorbereitungen für die Ausführung.

Wir freuen uns, dass Sie sich weiterhin auf die Wartung einer sicheren Netzwerkinfrastruktur konzentrieren. Bitte teilen Sie uns mit, wenn Sie weitere technische Informationen benötigen, indem Sie auf diese E-Mail antworten oder die bestehende Serviceanfrage stellen.

Mit freundlichen Grüßen
Cisco

In Outlook öffnen

① Verwenden Sie die .eml-Download unten. Ersetzen Sie alle **[Platzhalter in Klammern]** vor dem Senden.

✉ Outlook öffnen (nur Betreff)

📎 EML-Vorlage herunterladen

TAC 11-Vorlage ohne IOC für PSIRT2a/wurde nicht neu erstellt (**VORHER AUSGEFÜHRT**)

Anwendungsfall

Wird an Kunden gesendet, deren SD-WAN-Protokolle **keine Indicators of Compromise (IoCs)** im Zusammenhang mit dem PSIRT2a-Advisory aufweisen, UND die ihre Fabric **NICHT neu aufgebaut haben**. Bietet aktualisierte Anleitungen für die Problembehebung mit drei Optionen (Option 1 für die Nachbereitung).

Betreff

Dringende Maßnahmen erforderlich: SD-WAN Infrastructure Critical Vulnerability Remediation - SR [SR#]

Nachricht

Sehr geehrter Kunde,

vielen Dank, dass Sie das Cisco Technical Assistance Center (TAC) bezüglich der aktuellen PSIRT-Empfehlungen für das SD-WAN unter der Serviceanfrage [SR#] kontaktiert haben.

Nach der Überprüfung der Protokolle und Informationen aus Ihrer SD-WAN-Fabric konnten wir keine Indicators of Compromise (IOCs) identifizieren, die mit der Sicherheitslücke in SD-WAN vom 5. Juni 2026 in Verbindung stehen.

Wir verstehen auch, dass Ihre Umgebung nicht vollständig neu aufgebaut wurde, wie es die vorherigen Empfehlungen getan haben. Cisco empfiehlt, die nachstehenden aktualisierten Sanierungsleitfäden zu lesen, um das potenzielle Risiko zu verringern und die Integrität der Vertrauenskette für das SD-WAN-Zertifikat zu stärken.

Vor diesem Hintergrund stellen wir ein wichtiges Update für die Sanierung Ihrer SD-WAN-Fabric bereit, wie in [SR#] und den zuvor übermittelten Sicherheitsankündigungen beschrieben.

Während Sie sich bereits für einen Sanierungsplan basierend auf Option 1 entschieden haben, der ein Software-Upgrade und eine SSH-Schlüsselrotation beinhaltet, hat sich unsere Analyse der Bedrohungslandschaft weiterentwickelt. Neue technische Erkenntnisse über die Ausnutzung dieser Schwachstellen zeigen, dass dringend zusätzliche Maßnahmen ergriffen werden müssen, um das Risiko der Persistenz zu verringern und die Integrität der Zertifikatskette zu gewährleisten.

MASSNAHME ERFORDERLICH:

Wir haben die empfohlenen Wiederherstellungsstrategien aktualisiert, um einen umfassenderen Schutz durch die zusätzliche Rotation von Stammzertifikaten bereitzustellen.

Bitte beachten Sie, dass die Behebung zusätzliche Wartungsarbeiten erfordert, die geplante Netzwerkausfälle

einschließen können. Da Sicherheit und Integrität Ihres Netzwerks höchste Priorität haben, haben wir drei Optionen für die Problembeseitigung entwickelt. Jede der folgenden Optionen bietet ein ausgewogenes Verhältnis zwischen betrieblichen Auswirkungen und Sicherheitsgarantien. Da Ihr interner Risikostatus einzigartig ist, kann Cisco keinen bestimmten Pfad empfehlen.

Option A: Neubereitstellung mit rollendem Neustart. Zur Gewährleistung der Betriebskontinuität müssen Netzerkämpfe vermieden werden. Gleichzeitig bleibt das Risiko bestehen, dass die Bedrohung während des Übergangsprozesses anhält.

Beschreibung: Umfassende Controller-Neubereitstellung sowie SSH-Schlüssel- und Zertifikatsrotation. Bestehende Controller-Komponenten werden während der Migration über vManage zur Bereitstellung der neuen Fabric verbunden und nach der Migration des Geräts entfernt.

Option B: Umverteilung mit harter Umstellung. Bietet ein höheres Maß an Sicherheit. Da neue Controller nie mit alten Controllern verbunden werden, gibt es eine vollständige Isolierung. Dies hat Auswirkungen auf den gesamten Netzbetrieb, da alle Geräte die Verbindung wiederherstellen und Routen-/Verbindungsinformationen austauschen müssen. Die Ausfallzeit hängt von der Anzahl der Standorte, der ausgetauschten Präfixe usw. ab.

Beschreibung: Umfassende Controller-Neubereitstellung plus SSH-Schlüssel- und Zertifikatsrotation, aber die alten Controller-Komponenten werden während der Neubereitstellung von der neuen Fabric isoliert.

Option C: Vollständige Systemwiederherstellung Bietet ein Höchstmaß an Sicherheit durch die Erstellung einer sauberen Baseline. Dies ist jedoch der komplexeste Ansatz und birgt ein höheres Risiko konfigurationsbedingter Instabilität während der Wiederherstellung. Dies ist eine langwierige Option und erfordert Fachwissen beim Neuerstellen der Vorlagen- und Richtliniendatenbanken.

Wenn Ihr Team diese Optionen geprüft und den Ansatz ermittelt hat, der am besten zu Ihren Risikomanagementstandards passt, teilen Sie uns dies bitte mit, indem Sie auf diese Nachricht antworten. Nach Erhalt Ihrer Auswahl koordinieren wir das Wartungsfenster und beginnen die notwendigen technischen Vorbereitungen für die Ausführung.

Wir freuen uns, dass Sie sich weiterhin auf die Wartung einer sicheren Netzwerkinfrastruktur konzentrieren. Bitte teilen Sie uns mit, wenn Sie weitere technische Informationen benötigen, indem Sie auf diese E-Mail antworten oder die bestehende Serviceanfrage stellen.

Mit freundlichen Grüßen
Cisco

In Outlook öffnen

① Verwenden Sie die .eml-Download unten. Ersetzen Sie alle **[Platzhalter in Klammern]** vor dem Senden.

✉ Outlook öffnen (nur Betreff)

📎 EML-Vorlage herunterladen

TAC 12 Vorlage für yes IOC für PSIRT2a/they did not rebuild (**PREVIOUSLY IMPACTED**)

Anwendungsfall

Wird an Kunden gesendet, deren SD-WAN-Protokolle **Indicators of Compromise (IoCs)** im Zusammenhang mit dem PSIRT2a-Advisory zeigten UND die ihre Fabric **NICHT neu erstellt haben**. Bietet aktualisierte Anleitungen für die Problembehebung mit drei Optionen (Option 1 für die Nachbereitung).

Betreff

Dringende Maßnahmen erforderlich: SD-WAN Infrastructure Critical Vulnerability Remediation - SR [SR#]

Nachricht

Sehr geehrter Kunde,

vielen Dank, dass Sie das Cisco Technical Assistance Center (TAC) bezüglich der aktuellen PSIRT-Empfehlungen für das SD-WAN unter der Serviceanfrage [SR#] kontaktiert haben.

Nach der Analyse der Protokolle aus Ihrer SD-WAN-Fabric hat unser Team Indicators of Compromise (IOCs) identifiziert, die mit der Sicherheitslücke im SD-WAN vom 5. Juni 2026 in Verbindung stehen. Darüber hinaus haben wir Verständnis dafür, dass Ihre Umgebung nicht vollständig neu aufgebaut wurde, nachdem Sie zuvor entsprechende Empfehlungen abgegeben haben.

Angesichts dieser Indikatoren und der sich weiterentwickelnden Kenntnisse der Bedrohungslandschaft ist es wichtig, die unten aufgeführten aktualisierten Anleitungen zur Problembehebung zu überprüfen und zu implementieren, um das Persistenzrisiko zu reduzieren und die Integrität Ihrer SD-WAN-Zertifikatkette sicherzustellen.

Wir stellen ein wichtiges Update für die Sanierung Ihrer SD-WAN-Fabric bereit, wie in [SR#] und den zuvor übermittelten Sicherheitsankündigungen beschrieben. Diese Aktualisierung bezieht sich speziell auf Fabrics, in denen die übermittelten Protokolle Anzeichen für Indicators of Compromise (IOCs) aufwiesen.

Während Sie sich bereits für einen Sanierungsplan basierend auf Option 1 entschieden haben, der ein Software-Upgrade und eine SSH-Schlüsselrotation beinhaltet, hat sich unsere Analyse der Bedrohungslandschaft weiterentwickelt. Neue technische Erkenntnisse über die Ausnutzung dieser Schwachstellen zeigen, dass dringend zusätzliche Maßnahmen ergriffen werden müssen, um das Risiko der Persistenz zu verringern und die Integrität der Zertifikatskette zu gewährleisten.

MASSNAHME ERFORDERLICH:

Wir haben die empfohlenen Wiederherstellungsstrategien aktualisiert, um einen umfassenderen Schutz durch die zusätzliche Rotation von Stammzertifikaten bereitzustellen.

Bitte beachten Sie, dass die Behebung zusätzliche Wartungsarbeiten erfordert, die geplante Netzerkämpfe einschließen können. Da Sicherheit und Integrität Ihres Netzwerks höchste Priorität haben, haben wir drei Optionen für die Problembehebung entwickelt. Jede der folgenden Optionen bietet ein ausgewogenes Verhältnis zwischen betrieblichen Auswirkungen und Sicherheitsgarantien. Da Ihr interner Risikostatus einzigartig ist, kann Cisco keinen bestimmten Pfad empfehlen.

Option A: Neubereitstellung mit rollendem Neustart. Zur Gewährleistung der Betriebskontinuität müssen Netzerkämpfe vermieden werden. Gleichzeitig bleibt das Risiko bestehen, dass die Bedrohung während des Übergangsprozesses anhält.

Beschreibung: Umfassende Controller-Neubereitstellung sowie SSH-Schlüssel- und Zertifikatsrotation. Bestehende Controller-Komponenten werden während der Migration über vManage zur Bereitstellung der neuen Fabric verbunden und nach der Migration des Geräts entfernt.

Option B: Umverteilung mit harter Umstellung. Bietet ein höheres Maß an Sicherheit. Da neue Controller nie mit alten Controllern verbunden werden, gibt es eine vollständige Isolierung. Dies hat Auswirkungen auf den gesamten Netzbetrieb, da alle Geräte die Verbindung wiederherstellen und Routen-/Verbindungsinformationen austauschen müssen. Die Ausfallzeit hängt von der Anzahl der Standorte, der ausgetauschten Präfixe usw. ab.

Beschreibung: Umfassende Controller-Neubereitstellung plus SSH-Schlüssel- und Zertifikatsrotation, aber die alten Controller-Komponenten werden während der Neubereitstellung von der neuen Fabric isoliert.

Option C: Vollständige Systemwiederherstellung Bietet ein Höchstmaß an Sicherheit durch die Erstellung einer sauberen Baseline. Dies ist jedoch der komplexeste Ansatz und birgt ein höheres Risiko konfigurationsbedingter Instabilität während der Wiederherstellung. Dies ist eine langwierige Option und erfordert Fachwissen beim Neuerstellen der Vorlagen- und Richtliniendatenbanken.

Wenn Ihr Team diese Optionen geprüft und den Ansatz ermittelt hat, der am besten zu Ihren Risikomanagementstandards passt, teilen Sie uns dies bitte mit, indem Sie auf diese Nachricht antworten. Nach Erhalt Ihrer Auswahl koordinieren wir das Wartungsfenster und beginnen die notwendigen technischen Vorbereitungen für die Ausführung.

Wir freuen uns, dass Sie sich weiterhin auf die Wartung einer sicheren Netzwerkinfrastruktur konzentrieren. Bitte teilen Sie uns mit, wenn Sie weitere technische Informationen benötigen, indem Sie auf diese E-Mail antworten oder die bestehende Serviceanfrage stellen.

Mit freundlichen Grüßen

Cisco

In Outlook öffnen

① Verwenden Sie die .eml-Download unten. Ersetzen Sie alle **[Platzhalter in Klammern]** vor dem Senden.

✉ Outlook öffnen (nur Betreff)

📎 EML-Vorlage herunterladen

E-Mails für WAVE 2A für NEUE Kunden (bisher nicht betroffen)

TAC 13-Vorlage für kein IOC/kein festes Release verfügbar (WAVE 2a — Wartet auf Lösung)

Anwendungsfall

Wird an Kunden versendet, deren SD-WAN-Protokolle **keine Indicators of Compromise (IoCs)** im Zusammenhang mit CVE-2026-20245 aufwiesen, für die jedoch **derzeit keine feste Softwareversion** für ihre Plattform/Version **verfügbar ist**. Rät den Kunden, zwischenzeitliche Härtungsmaßnahmen anzuwenden und auf die Benachrichtigung über die feste Freigabe zu warten.

Betreff

Update: IoC-Bewertung abgeschlossen für CVE-2026-20245 - Derzeit keine feste Version verfügbar - SR [SR#]

Nachricht

Sehr geehrter Kunde,

vielen Dank, dass Sie sich für CVE-2026-20245 unter Service Request [SR#] an das Cisco Technical Assistance Center (TAC) wenden.

Wir haben die Analyse der Admin-Tech-Dateien abgeschlossen, die Sie von Ihren SD-WAN-Steuerungskomponenten bereitgestellt haben. **In den** untersuchten Protokollen **wurden keine Indicators of Compromise (IoCs)** im Zusammenhang mit CVE-2026-20245 **identifiziert**.

Bitte beachten Sie, dass die Menge der Protokolldaten, die im Rahmen dieser Prüfung abgerufen und an Cisco weitergegeben wurden, möglicherweise durch den Zeitraum begrenzt wurde, der gemäß dem [Cisco SD-WAN Hardening Guide](#) ^[1] in Ihrer Umgebung für die Aufbewahrung von Protokollen konfiguriert wurde.

Wichtig - Derzeit keine feste Softwareversion verfügbar:

Derzeit ist **keine feste Softwareversion** für Ihre aktuelle Plattform- und Softwareversion **verfügbar**, um diese Schwachstelle zu beheben. Die Techniker von Cisco arbeiten aktiv an der Bereitstellung einer festen Version. Sobald die Fixed-Software verfügbar ist, wird die [offizielle Sicherheitsempfehlung](#) ^[2] mit den Fixed-Versionsinformationen aktualisiert.

Empfohlene Zwischenmaßnahmen:

In Erwartung der Veröffentlichung des Updates empfehlen wir dringend die Implementierung der folgenden Härtingsmaßnahmen, um Ihr Risiko zu reduzieren:

1. **Best Practices für die Härtung anwenden:** Lesen Sie die Empfehlungen im [Cisco SD-WAN Hardening Guide](#)^[1] durch, und implementieren Sie sie, um Ihre Angriffsfläche zu verringern.
2. **Sicherheitsankündigung überwachen:** Überprüfen Sie regelmäßig die [offizielle Sicherheitsempfehlung](#)^[2] auf Updates zur Verfügbarkeit von festen Versionen für Ihre Plattform.
3. **Upgrade-Plan:** Beginnen Sie jetzt mit Ihrer Upgrade-Planung, damit Sie das Upgrade sofort ausführen können, sobald die feste Version veröffentlicht ist.
4. **Überwachung Ihrer Umgebung:** Überwachen Sie Ihre SD-WAN-Steuerungskomponenten weiterhin auf ungewöhnliches Verhalten oder unerwartete Konfigurationsänderungen.

Weitere Schritte:

Wir werden diesen Fall aktualisieren, sobald die feste Softwareversion verfügbar ist. An diesem Punkt sollten Sie das Upgrade aller SD-WAN-Steuerungskomponenten (Manager, Controller, Validator) auf die feste Version so schnell wie möglich priorisieren.

Wenn Sie ein BCS/LCS-Abonnement haben, wenden Sie sich an Ihren Cisco NCE oder Delivery Manager, um weitere Unterstützung bei der Upgrade-Planung zu erhalten.

Wir bedanken uns für Ihre Geduld und Ihr Engagement für die Sicherheit Ihrer Infrastruktur. Wenn Sie in der Zwischenzeit Fragen haben oder weitere Unterstützung benötigen, können Sie sich jederzeit an uns wenden.

Mit freundlichen Grüßen

Cisco Technical Assistance Center (TAC)

Links:

[1] [Cisco SD-WAN - Leitfaden zur Absicherung](#)

[2] [Offizielle Sicherheitsempfehlung \(cisco-sa-sdwan-privesc-4uxFrdzx\)](#)

In Outlook öffnen

① Ersetzen Sie alle **[Platzhalter in Klammern]** vor dem Senden.

✉ Outlook öffnen (nur Betreff)

⬇ EML-Vorlage herunterladen

TAC 14-Vorlage ohne IOC/Fixed Release verfügbar (WAVE 2a - Jetzt aktualisieren)

Anwendungsfall

Wird an Kunden gesendet, deren SD-WAN-Protokolle **keine Indicators of Compromise (IoCs)** im Zusammenhang mit CVE-2026-20245 aufwiesen, UND für die eine **feste Softwareversion verfügbar ist**. rät dem Kunden, die Planung und Ausführung des Upgrades sofort fortzusetzen.

Betreff

Update: IoC-Bewertung abgeschlossen für CVE-2026-20245 - keine IoCs gefunden, Upgrade erforderlich - SR [SR#]

Nachricht

Sehr geehrter Kunde,

vielen Dank, dass Sie sich für CVE-2026-20245 unter Service Request [SR#] an das Cisco Technical Assistance Center (TAC) wenden.

Wir haben die Analyse der Admin-Tech-Dateien abgeschlossen, die Sie von Ihren SD-WAN-Steuerungskomponenten bereitgestellt haben. **In den** untersuchten Protokollen **wurden keine Indicators of Compromise (IoCs)** im Zusammenhang mit CVE-2026-20245 **identifiziert**.

Bitte beachten Sie, dass die Menge der Protokolldaten, die im Rahmen dieser Prüfung abgerufen und an Cisco weitergegeben wurden, möglicherweise durch den Zeitraum begrenzt wurde, der gemäß dem [Cisco SD-WAN Hardening Guide](#) ^[1] in Ihrer Umgebung für die Aufbewahrung von Protokollen konfiguriert wurde.

Wichtig - Upgrade erforderlich:

Es wurden zwar keine IoCs identifiziert, die zugrunde liegende Schwachstelle bleibt jedoch bestehen, bis die SD-WAN-Steuerungskomponenten auf eine feste Softwareversion aktualisiert wurden. Eine fixe Version ist jetzt für Ihre Plattform verfügbar.

Priorisieren Sie Ihre Upgrade-Planung und -Durchführung als wichtigsten Schritt zur Behebung dieser Schwachstelle. Wenn Sie dieses Upgrade noch nicht geplant haben, führen Sie es bitte sofort durch.

Weitere Schritte:

- 1. Upgrade aller Komponenten der SD-WAN-Steuerung:** Aktualisieren Sie Ihren Manager (vManage), Controller (vSmart) und Validator (vBond) auf eine feste Softwareversion, die in der [offiziellen Sicherheitsempfehlung](#) aufgeführt ist ^[2].
- 2. Upgrade-Ressourcen:** Detaillierte Anweisungen zum Upgrade finden Sie in den folgenden offiziellen Cisco Dokumenten:
 - [Starten Sie Ihr Catalyst SD-WAN-Upgrade](#) ^[3]
 - [Cisco SD-WAN-Upgrade-Leitfaden](#) ^[4]
- 3. Ticketabschluss:** Sobald Sie das Software-Upgrade für Ihre gesamte Umgebung erfolgreich abgeschlossen haben, können Sie in Erwägung ziehen, diesen Fall zu beheben und mit den Standardverfahren zur Schließung fortzufahren.

Wenn Sie ein BCS/LCS-Abonnement haben, wenden Sie sich an Ihren Cisco NCE oder Delivery Manager, um weitere Unterstützung beim Upgrade zu erhalten.

Wir werden Ihren Fall weiterhin überwachen. Wenn wir innerhalb von 10 Geschäftstagen keine Rückmeldung erhalten, gehen wir davon aus, dass keine weitere Unterstützung erforderlich ist, und fahren mit den normalen TAC-Verfahren zum Fallabschluss fort.

Mit freundlichen Grüßen

Cisco Technical Assistance Center (TAC)

Links:

[1] [Cisco SD-WAN - Leitfaden zur Absicherung](#)

[2] [Offizielle Sicherheitsempfehlung \(cisco-sa-sdwan-privesc-4uxFrdzx\)](#)

[3] [Starten Sie Ihr Catalyst SD-WAN-Upgrade](#)

[4] [Cisco SD-WAN-Upgrade-Leitfaden](#)

In Outlook öffnen

📘 Ersetzen Sie alle **[Platzhalter in Klammern]** vor dem Senden.

📧 Outlook öffnen (nur Betreff)

📎 EML-Vorlage herunterladen

TAC 15-Vorlage für identifizierte/feste IOC-Version verfügbar (WAVE 2a — dringendes Upgrade)

Anwendungsfall

Wird an Kunden gesendet, deren SD-WAN-Protokolle **Indicators of Compromise (IoCs)** im Zusammenhang mit CVE-2026-20245 zeigten UND für die eine **feste Softwareversion verfügbar ist**. Der Kunde wird aufgefordert, dringend ein Upgrade durchzuführen und einen Überprüfungsanruf zu vereinbaren, um die Ergebnisse und die Beseitigung zu besprechen.

Betreff

DRINGEND: IoC identifiziert für CVE-2026-20245 - sofortiges Upgrade erforderlich - SR [SR#]

Nachricht

Sehr geehrter Kunde,

vielen Dank, dass Sie sich für CVE-2026-20245 unter Service Request [SR#] an das Cisco Technical Assistance Center (TAC) wenden.

Nach der Analyse der Admin-Tech-Dateien, die von Ihren SD-WAN-Steuerungskomponenten bereitgestellt werden, hat unser Team **Indicators of Compromise (IoCs)** im Zusammenhang mit CVE-2026-20245 **identifiziert**.

Angesichts der Art dieser Ergebnisse ist es von entscheidender Bedeutung, dass wir die technischen Details und die empfohlenen nächsten Schritte so bald wie möglich erörtern. Gerne vereinbaren wir mit Ihrem Team einen Termin für ein Gespräch, um die Ergebnisse genauer zu besprechen und die geeignete Vorgehensweise zur Problembehebung zu besprechen.

Sofortmaßnahmen erforderlich:

1. **Sofortiges Upgrade der SD-WAN-Steuerungskomponenten:** Für Ihre Plattform steht eine feste Softwareversion zur Verfügung. Aktualisieren Sie Ihren Manager (vManage), Controller (vSmart) und Validator (vBond) so bald wie möglich auf eine feste Softwareversion, die in der [offiziellen Sicherheitsempfehlung](#) ^[1] aufgeführt ist. Das Upgrade schließt die Schwachstelle sofort.
2. **Anruf vereinbaren:** Teilen Sie uns bitte mit, ob Sie innerhalb der nächsten [z. B. 4-8 Stunden] für einen kurzen Anruf bereit sind, um die Ergebnisse des IoC zu überprüfen und die empfohlenen Optionen zur Problembehebung zu besprechen.
3. **Best Practices für die Härtung anwenden:** Lesen Sie die Empfehlungen im [Cisco SD-WAN Hardening Guide](#) ^[2] durch, und implementieren Sie sie, um die Angriffsfläche zu verringern, während eine Beseitigung geplant ist.

Upgrade-Ressourcen:

- [Starten Sie Ihr Catalyst SD-WAN-Upgrade](#) ^[3]
- [Cisco SD-WAN-Upgrade-Leitfaden](#) ^[4]

Wichtig: Im Anschluss an das Upgrade werden möglicherweise weitere Korrekturmaßnahmen empfohlen (z. B. erneute Bereitstellung des Controllers und Rotation des Zertifikats), je nach Schweregrad der identifizierten Kompromittierung. Diese werden während des Überprüfungsaufrufs erörtert.

Detaillierte Optionen zur Problembehebung finden Sie im [TAC](#)-Behebungshandbuch ^[5].

Unser vorrangiges Ziel ist es, Sie bei der Sicherung Ihrer Umgebung und der Minderung potenzieller Risiken zu unterstützen. Wir freuen uns, dass Sie sich umgehend mit dieser Angelegenheit befassen und uns mit Ihnen abstimmen werden.

Mit freundlichen Grüßen

Cisco Technical Assistance Center (TAC)

Links:

[1] [Offizielle Sicherheitsempfehlung \(cisco-sa-sdwan-privesc-4uxFrdzx\)](#)

[2] [Cisco SD-WAN - Leitfaden zur Absicherung](#)

[3] [Starten Sie Ihr Catalyst SD-WAN-Upgrade](#)

[4] [Cisco SD-WAN-Upgrade-Leitfaden](#)

[5] [TAC-Sanierungsleitfaden](#)

In Outlook öffnen

① Ersetzen Sie alle **[Platzhalter in Klammern]** vor dem Senden.

✉ Outlook öffnen (nur Betreff)

⬇ EML-Vorlage herunterladen

TAC 16-Vorlage für IOC identifiziert/keine feste Version verfügbar (WAVE 2a — Harden & Await Fix)

Anwendungsfall

Wird an Kunden gesendet, deren SD-WAN-Protokolle **Indicators of Compromise (IoCs)** im Zusammenhang mit CVE-2026-20245 zeigten, für die **derzeit jedoch keine feste Softwareversion** für ihre Plattform/Version **verfügbar ist**. Beratung zur sofortigen Härtung, Planung eines Überprüfungsgesprächs und Informierung des Kunden, dass er auf die Behebung der Probleme durch die feste Version warten muss.

Betreff

DRINGEND: IoC identifiziert für CVE-2026-20245 - Derzeit keine feste Version verfügbar - SR [SR#]

Nachricht

Sehr geehrter Kunde,

vielen Dank, dass Sie sich für CVE-2026-20245 unter Service Request [SR#] an das Cisco Technical Assistance Center (TAC) wenden.

Nach der Analyse der Admin-Tech-Dateien, die von Ihren SD-WAN-Steuerungskomponenten bereitgestellt werden, hat unser Team **Indicators of Compromise (IoCs)** im Zusammenhang mit CVE-2026-20245 **identifiziert**.

Angesichts der Schwere dieser Feststellungen ist es von entscheidender Bedeutung, dass wir die technischen Einzelheiten und die empfohlenen Zwischenmaßnahmen so bald wie möglich erörtern. Wir würden gerne einen Termin mit Ihrem Team vereinbaren, um die Ergebnisse zu besprechen.

Wichtig - Derzeit keine feste Softwareversion verfügbar:

Derzeit ist **keine feste Softwareversion** für Ihre aktuelle Plattform- und Softwareversion **verfügbar**, um diese Schwachstelle vollständig zu beheben. Die Techniker von Cisco arbeiten aktiv an der Bereitstellung einer festen Version. Sobald die Fixed-Software verfügbar ist, wird die [offizielle Sicherheitsempfehlung](#) ^[1] mit den Fixed-Versionsinformationen

aktualisiert.

Sofortmaßnahmen erforderlich:

1. **Anruf vereinbaren:** Bitte teilen Sie uns mit, ob Sie innerhalb der nächsten [z. B. 4-8 Stunden] einen kurzen Anruf erhalten, um die IoC-Ergebnisse zu überprüfen und vorläufige Eindämmungsmaßnahmen zu besprechen.
2. **Sofortige Anwendung der Best Practices für die Härtung:** Lesen Sie die Empfehlungen im [Cisco SD-WAN Hardening Guide](#)^[2] durch, und implementieren Sie sie, um die Angriffsfläche in Erwartung der Veröffentlichung des Updates zu reduzieren.
3. **Erweiterte Überwachung:** Überwachen Sie Ihre SD-WAN-Steuerungskomponenten genau auf ungewöhnliches Verhalten, unerwartete Konfigurationsänderungen oder nicht autorisierte Zugriffsversuche.
4. **Sicherheitsankündigung überwachen:** Überprüfen Sie regelmäßig die [offizielle Sicherheitsempfehlung](#)^[1] auf Updates zur Verfügbarkeit von festen Versionen für Ihre Plattform.
5. **Upgrade-Plan:** Beginnen Sie jetzt mit Ihrer Upgrade-Planung, damit Sie das Upgrade sofort ausführen können, sobald die feste Version veröffentlicht ist.

Weitere Schritte:

Wir werden diesen Fall aktualisieren, sobald die feste Softwareversion verfügbar ist. An diesem Punkt müssen Sie das Upgrade aller SD-WAN-Steuerungskomponenten (Manager, Controller, Validator) auf die feste Version sofort priorisieren. Im Anschluss an das Upgrade werden basierend auf den Ergebnissen unseres Gesprächs weitere Schritte zur Problembehebung besprochen (z. B. die Neubereitstellung des Controllers und die Rotation der Zertifikate).

Weitere Informationen zu den Optionen zur Problembehebung finden Sie im [TAC-Behebungshandbuch](#) ^[3], das verfügbar wird, sobald die feste Version verfügbar ist.

Unser vorrangiges Ziel ist es, Sie bei der Sicherung Ihrer Umgebung und der Minderung potenzieller Risiken zu unterstützen. Wir freuen uns, dass Sie sich umgehend mit dieser Angelegenheit befassen und uns mit Ihnen abstimmen werden.

Mit freundlichen Grüßen

Cisco Technical Assistance Center (TAC)

Links:

[1] [Offizielle Sicherheitsempfehlung \(cisco-sa-sdwan-privesc-4uxFrzx\)](#)

[2] [Cisco SD-WAN - Leitfaden zur Absicherung](#)

[3] [TAC-Sanierungsleitfaden](#)

ⓘ Ersetzen Sie alle **[Platzhalter in Klammern]** vor dem Senden.

✉ Outlook öffnen (nur Betreff)

↓ EML-Vorlage herunterladen

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.