Sicherheitshinweis für Catalyst SD-WAN - Mai 2026

Inhalt

Einleitung

In diesem Dokument werden die Schritte zur Identifizierung und Behebung kritischer Sicherheitslücken in SD-WAN auf der Grundlage der PSIRT-Empfehlungen vom 14. Mai 2026 beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Catalyst SD-WAN-Architektur und Steuerungskomponenten (vManage, vSmart, vBond)
- Cisco Catalyst SD-WAN-Upgrade-Verfahren
- Cisco TAC-Fallmanagement und Verfahren zur Erfassung von Admin-Tech-Daten

Verwendete Komponenten

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Detaillierte Hintergrundinformationen und die neuesten Updates finden Sie auf der offiziellen PSIRT-Beratungs-Seite.

Diese Ankündigungen finden Sie unter folgenden Links:

- Sicherheitslücke bei Cisco Catalyst SD-WAN-Controller-Authentifizierung umgangen
- Sicherheitslücken in Cisco Catalyst SD-WAN

Diese Mängel werden durch folgende PSIRT-Ankündigungen behoben:

- Cisco Bug-ID CSCwt50498
- Cisco Bug-ID CSCwt38739
- Cisco Bug-ID CSCwt38767
- Cisco Bug-ID CSCwt55544

Behebungs-Workflow - Übersicht

Anmerkung: Alle SD-WAN-Controller und -Manager sind anfällig und erfordern ein sofortiges Upgrade aller Steuerungskomponenten. Nicht alle Controller weisen jedoch einen Kompromittierungsnachweis auf.

Erforderliche Aktion: Sammeln Sie Admin-Techniker, aktualisieren Sie auf eine feste Version, und öffnen Sie dann ein Cisco TAC-Ticket, damit TAC Ihre Admin-Techniker nach Indications of Compromise durchsuchen kann.

Das TAC ist verfügbar für:

- Durchsuchen Sie die von Ihnen bereitgestellten Admin-Technologien nach Anzeichen für eine Kompromittierung.
- Upgrade-Support bei Problemen während des Upgrades
- Zusätzliche Korrekturmaßnahmen durchführen, wenn Anzeichen für eine Kompromittierung erkannt werden

1. Collect Admin-Tech - Führen Sie admin-tech auf allen Steuerungskomponenten (vSmart, vManage, vBond) vor dem Upgrade aus, um sicherzustellen, dass keine Diagnosedaten

verloren gehen. Wählen Sie Log- und Tech-Optionen aus. Core ist nicht erforderlich.

Vorsicht: vSmart admin-techs darf nicht gleichzeitig ausgeführt werden, sondern muss einzeln ausgeführt werden. Alle anderen können in beliebiger Reihenfolge gesammelt werden

2. Upgrade auf eine feste Version - Führen Sie für alle SD-WAN-Steuerungskomponenten (vManage, vSmart, vBond) ein Upgrade auf eine feste Softwareversion durch, die in der Tabelle mit festen Softwareversionen aufgeführt ist.

Anmerkung: Warten Sie nicht vor dem Upgrade auf die Ergebnisse des TAC-Scans. Das Upgrade auf eine feste Version hat höchste Priorität und schließt die Schwachstelle. Der TAC-Scan in Schritt 3 bestimmt, ob nach dem Upgrade weitere Maßnahmen erforderlich sind.

3. TAC-Ticket öffnen und Admin-Tech hochladen, um nach Indicators of Compromise zu suchen - Öffnen Sie ein Cisco TAC-Ticket, und laden Sie alle in Schritt 1 erfassten Admin-Tech-Protokollpakete hoch. TAC durchsucht die Admin-Tech nach Indications of Compromise.
4. Wenn eine Kompromittierung erkannt wurde, befolgen Sie die TAC-Richtlinien. Wenn das TAC Indicators of Compromise in Ihrer Umgebung identifiziert, befolgen Sie alle vom TAC bereitgestellten Anweisungen zur Problembehebung. Wenn keine Anzeichen für eine Kompromittierung gefunden werden, sind über das Upgrade hinaus keine weiteren Maßnahmen erforderlich.

Schritt 1: Admin-Tech-Dateien von allen Steuerungskomponenten sammeln

Erforderlich: Sammeln Sie vor dem Upgrade Admin-Tech-Dateien von allen Steuerungskomponenten, um sicherzustellen, dass keine Diagnosedaten verloren gehen. Diese Dateien werden vom TAC in Schritt 3 verwendet, um Ihre Umgebung auf Anzeichen einer Kompromittierung zu durchsuchen.

Sammlung:

Anmerkung: Wählen Sie für die Administrator-Tech-Erstellung die Optionen Log (Protokoll) und Tech (Technologie). Core ist nicht erforderlich.

1. Führen Sie admin-tech auf ALLEN Controllern (vSmarts) aus - führen Sie diese nicht gleichzeitig aus. eine nach der anderen abholen
2. Admin-Tech auf ALLEN Managern (vManages) ausführen

3. Admin-Tech auf ALLEN Validatoren (vBonds) ausführen

Anmerkung: vSmart-Admin-Technik darf nicht gleichzeitig ausgeführt werden, sondern muss einzeln abgefragt werden. Admin-Technik für Manager und Validatoren kann in beliebiger Reihenfolge gesammelt werden.

Admin-Tech in SD-WAN-Umgebung erfassen und auf TAC-Ticket hochladen

Anmerkung: Das TAC analysiert diese Dateien, um Ihre Umgebung auf Anzeichen für Kompromittierung zu untersuchen und den entsprechenden Sanierungspfad festzulegen.

Alternative: Manuelle Überprüfung (nur wenn Admin-Tech nicht erfasst werden kann)

Für Benutzer, die keine Admin-Tech-Dateien freigeben können, stehen manuelle Überprüfungsschritte zur Verfügung. Diese Schritte enthalten vorläufige Indikatoren, die dokumentiert und an das TAC weitergegeben werden müssen.

Detaillierte Anweisungen hierzu finden Sie im Abschnitt "Manuelle Verifizierung" am Ende dieses Dokuments. Dokumentieren Sie alle Ergebnisse, und stellen Sie sie dem TAC in Ihrem Supportfall zur Verfügung.

Phase 2: Upgrade auf eine feste Softwareversion

Nachdem Sie in Schritt 1 die Admin-Technik erfasst haben, aktualisieren Sie alle SD-WAN-Steuerungskomponenten (vManage, vSmart und vBond) auf eine feste Softwareversion.

Wichtig: Warten Sie nicht vor dem Upgrade auf die Ergebnisse des TAC-Scans. Das Upgrade auf eine feste Version hat höchste Priorität und schließt die Schwachstelle. Der TAC-Scan in Schritt 3 bestimmt, ob nach dem Upgrade weitere Maßnahmen erforderlich sind.

Wählen Sie in der Tabelle Fixed Software Versions (Feste Softwareversionen) in diesem Dokument die entsprechende Version aus.

Warnung: Das Upgrade muss innerhalb Ihrer aktuellen Hauptversion bleiben. Führen Sie ohne ausdrückliche Anleitung des TAC kein Upgrade auf eine höhere Hauptversion durch.

Upgrade von SD-WAN-Controllern mithilfe der vManage-GUI oder -CLI

Anmerkung: Wenn während des Upgrades Probleme auftreten, öffnen Sie ein TAC-Ticket für Upgrade-Support.

Schritt 3: TAC-Ticket öffnen und Admin-Tech-Dateien zum Scannen hochladen

Öffnen Sie nach dem Upgrade in Schritt 2 ein Cisco TAC-Support-Ticket, und laden Sie die in Schritt 1 erfassten Admin-Tech-Dateien hoch. TAC überprüft die Admin-Techniker auf Anzeichen für eine Kompromittierung.

Erforderliche Aktionen:

1. Öffnen Sie ein TAC-Ticket mit Schweregrad 3, "CVE-2026-20182" und der entsprechenden PSIRT-ID im Titel, um den Scanvorgang einzuleiten.
2. Laden Sie ALLE in Schritt 1 gesammelten Admin-Tech-Protokollpakete hoch (Controller, Manager und Prüfer).
3. Warten Sie, bis das TAC den Scan abgeschlossen hat, und teilen Sie die Ergebnisse mit.

Anmerkung: TAC analysiert die Admin-Tech Dateien und teilt die Ergebnisse des Scans mit. Wenn keine Anzeichen für eine Kompromittierung gefunden werden, sind über das Upgrade hinaus keine weiteren Maßnahmen erforderlich.

Schritt 4: Bei Erkennung eines Kompromittierens - TAC-Richtlinien befolgen

Wenn das TAC Anzeichen für eine Kompromittierung in Ihrer Umgebung identifiziert, setzt sich das TAC mit Ihnen in Verbindung und hilft Ihnen bei der Problembehebung. Befolgen Sie alle Anweisungen des TAC.

Wenn keine Anzeichen für eine Kompromittierung erkannt werden, ist das in Schritt 2 abgeschlossene Upgrade ausreichend, und es ist keine weitere Behebung erforderlich.

Fest implementierte Softwareversionen

Diese Softwareversionen enthalten Korrekturen für die identifizierten Schwachstellen:

Gilt für aktuelle Versionen	Feste Version	Verfügbare Software
20,3, 20,6, 20,9	20.9.9.1	20.9.9.1 Upgrade-Images für vManage, vSmart und vBond
20.10, 20.11, 20.12.5 und frühere Versionen in 20.12	20.12.5.4	20.12.5.4 Upgrade-Images für vManage, vSmart und vBond
20.12.6.x	20.12.6.2	20.12.6.2 Upgrade-Images für vManage, vSmart und vBond
20.12.7	20.12.7.1	20.12.7.1 Upgrade-Images für vManage, vSmart und vBond
20.13, 20.14, 20.15.4.3 und früher in 20.15	20.15.4.4	20.15.4.4 Upgrade-Images für vManage, vSmart und vBond
20.15.5.x	20.15.5.2	20.15.5.2 Upgrade-Images für vManage, vSmart und vBond
20.16, 20.17, 20.18.x	20.18.2.2	20.18.2.2 Upgrade-Images für vManage, vSmart und vBond

Hinweis: Für Kunden, die in der SD-WAN-Cloud (früher bekannt als Cloud Delivered Cisco Catalyst SD-WAN [CDCS]) arbeiten, ist der Release 20.15.506 ebenfalls ein fester Bestandteil. Dies gilt speziell für die von Cisco gehostete Cluster-Bereitstellung und wird getrennt vom Standard-Upgrade-Pfad behandelt. Für alle diese Kunden wurde bereits ein Upgrade auf die feste Version 20.15.506 durchgeführt.

Wichtige Hinweise:

- Upgrade-Matrix
- Controller-Kompatibilitätsmatrix

Anhang: Manuelle Verifizierungsschritte (nur wenn Admin-Tech-Erfassung nicht möglich)

Anmerkung: Die Sammlung von Admin-Tech ist die bevorzugte und empfohlene Methode. Verwenden Sie nur dann eine manuelle Überprüfung, wenn Sie keine admin-tech-Dateien

sammeln und weitergeben können. Wenn Sie keine Admin-Tech-Dateien sammeln können, verwenden Sie diese manuellen Schritte, um vorläufige Indikatoren für das TAC zu sammeln.

Anmerkung:

- Diese Schritte stellen nur vorläufige Daten bereit.
- Eine Sammlung von Admin-Tech-Artikeln ist für eine genaue Bewertung sehr zu bevorzugen.
- Dokumentieren Sie Ihre Erkenntnisse, und geben Sie sie an das TAC in Ihrem Supportfall weiter.
- Die TAC legt die offizielle Bewertung fest

Anforderungen: Diese Schritte müssen an allen Steuerungskomponenten durchgeführt werden.

Überprüfung 1: Suchen nach nicht autorisierten SSH-Anmeldungen in Auth-Protokollen

Schritt 1: Identifizieren gültiger vManage-System-IPs

Zugriff auf jeden vSmart Controller und Ausführung:

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

Beispiel:

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

Phase 2: Zeichenfolge für regulären Ausdruck erstellen (nur vBond und vSmart)

Alle System-IPs aus Schritt 1 in einem OR-Regex-Muster kombinieren:

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

Schritt 2b: Zusätzlicher Schritt für vManage-Systeme

Wenn diese Befehle auf vManage selbst ausgeführt werden, fügen Sie die IP-Adresse des lokalen Hosts (127.0.0.1), die IP-Adresse des lokalen Systems, alle Cluster-IPs und die IP-Adresse der VPN 0-Transportschnittstelle an den regulären Ausdruck an:

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

Um die lokale IP-Adresse des vManage-Systems zu finden, verwenden Sie:

```
show control local-properties
```

Um die IP- und Cluster-IP-Adresse der VPN 0-Transportschnittstelle zu finden, verwenden Sie:

```
show interface | tab
```

Schritt 3: Verifizierungsbefehl ausführen

Führen Sie diesen Befehl aus, und ersetzen Sie REGEX durch Ihre reguläre Zeichenfolge aus Schritt 2:

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

Anmerkung: Mit diesem Befehl werden Authentifizierungsprotokolle gefiltert, sodass nur vmanage-admin-Anmeldungen von unerwarteten Quellen angezeigt werden. Legitime Anmeldungen dürfen nur von IPs stammen, die mit vManage in Verbindung stehen.

Schritt 4: Interpretation der Ergebnisse und Dokumentation für das TAC

Wenn KEINE Ausgabe angezeigt wird:

- Keine Indications of Compromise auf diesem Gerät erkannt
- Dokumentieren Sie dieses Ergebnis für Ihren TAC-Ticket.
- Bewertung der verbleibenden Controller fortsetzen

Wenn Protokollzeilen gedruckt werden:

- Überprüfen Sie sorgfältig alle angezeigten IP-Adressen.
- Überprüfen Sie, ob die IP-Adresse nicht mit der vManage-Infrastruktur (Cluster-IP, alte System-IP-Adresse oder Ähnliches) zusammenhängt.
- Wenn Sie die Quell-IP nicht als legitim identifizieren können, kann dies auf potenzielle Indications of Compromise hinweisen.
- Der Protokolleintrag zeigt einen Zeitstempel und eine Quell-IP-Adresse an
- Dokumentieren Sie alle Ergebnisse, und eröffnen Sie sofort ein TAC-Ticket.
- Integrieren Sie die Protokolleinträge, Zeitstempel und Quell-IPs in Ihrem Ticket.
- TAC führt offizielle Bewertungsbestimmung durch

Überprüfung 2: Suchen nach nicht autorisierten Peer-Verbindungen in Controller-Syslogs

Dieser Befehl extrahiert alle Peer-Typ- und Peer-System-IP-Paare aus den Syslog-Dateien des Controllers und gibt sie als Liste aus, die Sie überprüfen können. Verdächtige Einträge werden nicht automatisch gekennzeichnet. Sie müssen die Ausgabe überprüfen und feststellen, ob jede IP-Adresse des Peer-Systems ein bekannter, legitimer Teil Ihrer SD-WAN-Infrastruktur ist. Führen Sie diesen Vorgang für alle Steuerelementkomponenten aus (Controller, Manager und Validatoren).

Schritt 1: Führen Sie den Befehl für jede Steuerelementkomponente aus:

Rufen Sie zunächst vshell auf, und navigieren Sie zum Protokollverzeichnis:

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

Führen Sie dann diesen Befehl aus, um die vsyslog*-Dateiglob zu durchsuchen:

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

Wiederholen Sie dies für messages* file glob und vdebug* file glob.

Phase 2: Interpretation der Ergebnisse und Dokumentation für das TAC

Wenn die Ausgabe nur bekannte IPs des vManage/vSmart/vBond-Systems anzeigt:

- Bei dieser Prüfung wurden keine Anzeichen für eine Kompromittierung erkannt.
- Dokumentieren Sie dieses Ergebnis für Ihren TAC-Ticket.
- Bewertung der verbleibenden Steuerungskomponenten fortsetzen

Wenn die Ausgabe nicht erkannte IPs des Peer-Systems enthält:

- Überprüfen Sie sorgfältig alle abgebildeten IP-Adressen und Peer-Typen.
- Vergewissern Sie sich, dass die IP nicht mit Ihrer bekannten SD-WAN-Kontrollebeneninfrastruktur in Zusammenhang steht.
- Wenn Sie die Quell-IP nicht als legitim identifizieren können, kann dies auf potenzielle Indications of Compromise hinweisen.
- Dokumentieren Sie alle Ergebnisse, und eröffnen Sie sofort ein TAC-Ticket.
- Integrieren Sie die vollständige Befehlsausgabe mit Peer-Typ- und Peer-System-IP-Paaren in Ihrem Fall.
- TAC führt offizielle Bewertungsbestimmung durch

Überprüfung 3: Überprüfen Sie die aktiven Steuerverbindungen auf fehlende Challenge-Back.

Bei dieser Prüfung werden die detaillierten Ergebnisse der Kontrollverbindungen für Peer-Sitzungen überprüft, die als aktiv (oder kürzlich abgebrochen) gemeldet werden, aber den erwarteten `Challenge-Back-`Austausch nicht aufweisen. Eine Sitzung, in der Datenpakete in beide Richtungen ausgetauscht werden, während gleichzeitig `Challenge-ack 0` in den Tx- oder Rx-Statistiken angezeigt wird, deutet darauf hin, dass der Peer den erwarteten Challenge-Handshake nie abgeschlossen hat. Diese Anomalie rechtfertigt eine Untersuchung. Führen Sie diesen Vorgang für alle Steuerelementkomponenten aus (Controller, Manager und Validatoren).

Schritt 1: Sammeln Sie die Steuerungsanschlüsse Detailausgabe

Führen Sie in der Geräte-CLI Folgendes aus:

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

Speichern Sie die Ausgabe in einer Datei (z. B. `vdaemon.txt`) zur Überprüfung.

Phase 2: Zu suchende Elemente

Markieren Sie für jeden Peer-Datensatz (durch `REMOTE-COLOR-`/`SYSTEM-IP-`Header getrennt) den Datensatz, wenn alle dieser Bedingungen zutreffen:

- Sitzungsstatus ist UP oder TEAR_DOWN
- Sowohl der Tx Statistics Hello Zähler als auch der Rx Statistics Hello Zähler sind ungleich null (Hellos fließen in beide Richtungen)

- Challenge-ack ist 0 im Block Tx Statistics oder Rx Statistics (oder beiden).

Beispiel für einen passenden Datensatz (beachten Sie die Pfeile `<<<`, die das fehlende `Challenge-ack` markieren)

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

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

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

Im obigen Beispiel sind sowohl die Tx- als auch die Rx-`Hello`-Zähler ungleich null (aktive Verbindung), aber `das Challenge-Back` ist in beiden Richtungen `0`.

Schritt 3: Manueller Suchbefehl

Führen Sie Folgendes aus, um Kandidatendatensätze schnell aus einer gespeicherten `Datei vdaemon.txt (`oder aus einer beliebigen Datei, die die Ausgabe von `show control connections detail` enthält) aufzudecken:

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

Jeder zurückgegebene Block stellt eine Peer-Sitzung dar, bei der das Challenge-Back als 0 gemeldet wird. Überprüfen Sie jeden Block vollständig, um sicherzustellen, dass der Status `up`

oder `tear_down` ist, und dass die `Hello`-Zähler sowohl in Tx als auch in Rx ungleich null sind, bevor er als Treffer behandelt wird.

Schritt 4: Interpretation der Ergebnisse und Dokumentation für das TAC

Wenn keine Datensätze alle drei Bedingungen erfüllen:

- Bei dieser Prüfung wurden keine Anzeichen für eine Kompromittierung erkannt.
- Dokumentieren Sie dieses Ergebnis für Ihren TAC-Ticket.
- Bewertung der verbleibenden Steuerungskomponenten fortsetzen

Wenn ein oder mehrere Datensätze alle drei Bedingungen erfüllen:

- Überprüfen Sie sorgfältig die Werte `SYSTEM-IP-`, `private-ip` und `public-ip` für jeden markierten Datensatz.
- Überprüfen Sie, ob der Peer kein bekannter und legitimer Teil Ihrer SD-WAN-Kontrollebene ist (Clustermitglied, DR-Standort, IP-Adresse, die zuvor einer Komponente zugewiesen war).
- Wenn Sie den Peer nicht als legitim identifizieren können, kann dies auf potenzielle Anzeichen für eine Kompromittierung hinweisen.
- Dokumentieren Sie alle Ergebnisse, und eröffnen Sie sofort ein TAC-Ticket.
- Integrieren Sie den (die) vollständigen Peer-Datensatz(e) und die Ausgabe des Quellbefehls in Ihrem Fall.
- TAC führt offizielle Bewertungsbestimmung durch

Häufig gestellte Fragen

F: Was ist der erste Schritt, um diese Sicherheitsempfehlung umzusetzen?

A : Sammeln Sie Admin-Tech-Dateien von allen Steuerungskomponenten, und aktualisieren Sie dann alle Steuerungskomponenten auf eine feste Softwareversion. Öffnen Sie nach dem Upgrade ein TAC-Ticket, und laden Sie die Admin-Techniker hoch, damit TAC Ihre Umgebung auf Anzeichen für eine Kompromittierung durchsuchen kann.

Frage: Welche Version benötige ich für ein Upgrade?

A. Bitte aktualisieren Sie frühestens auf die nächstgelegene feste Version.

F: Muss ich Admin-Techniker von allen Steuerungskomponenten sammeln?

A : Ja, das TAC erfordert Admin-Tech-Dateien von allen Controllern (vSmart, jeweils eine erfasst), allen Managern (vManage) und allen Validatoren (vBond), um Ihre Umgebung richtig zu bewerten.

F: Wie ermittelt das TAC, ob mein System kompromittiert wurde?

A : Das TAC analysiert die Admin-Tech-Dateien mithilfe spezieller Tools, um Ihre Umgebung auf Anzeichen für eine Kompromittierung zu untersuchen.

F: Kann ich meine eigene automatische Suche mit TAC-Tools durchführen?

A : Kunden können auch das Self-Service-Tool "Check Bug Applicability" verwenden, das auf der Bug Search Tool-Seite für die Cisco Bug-ID CSCwt50498 integriert ist, um Admin-Techniker aus den Steuerungskomponenten erneut zu scannen.

F: Was passiert, wenn Anzeichen für eine Kompromittierung erkannt werden?

A : TAC kontaktiert Sie, um die nächsten Schritte und spezifische Richtlinien für Ihre Umgebung zu besprechen. Cisco führt die Fehlerbehebung nicht in Ihrem Namen durch - das TAC bietet Ihnen die nötigen Anleitungen für die Vorgehensweise.

F: Woher weiß ich, welche feste Softwareversion ich verwenden soll?

A : Weitere Informationen finden Sie in der Tabelle Fixed Software Versions in diesem Dokument. TAC bestätigt die für Ihre spezifische Umgebung passende Version.

F: Kann ich das Upgrade starten, bevor das TAC meine Admin-Techniker analysiert?

A : Ja. Erfassen Sie Admin-Techniker, aktualisieren Sie auf eine feste Version, und öffnen Sie dann ein TAC-Ticket, damit das TAC die Admin-Techniker auf Anzeichen für eine Kompromittierung untersuchen kann.

F: Sind Ausfallzeiten während der Problembehebung zu erwarten?

A : Die Auswirkungen hängen von Ihrer Bereitstellungsarchitektur und dem Wiederherstellungspfad ab. Das TAC bietet Hilfestellung bei der Minimierung der Auswirkungen auf den Service während des Prozesses.

F: Müssen alle Controller aktualisiert werden, wenn keine Anzeichen für eine Kompromittierung gefunden werden?

A : Ja, alle SD-WAN-Steuerungskomponenten (vManage, vSmart und vBond) müssen auf eine feste Softwareversion aktualisiert werden. Ein Upgrade nur einer Untergruppe von Controllern ist nicht ausreichend.

F: Ich habe ein Cloud-gehostetes SD-WAN-Overlay. Welche Upgrade-Optionen stehen zur Verfügung?

A : Für in der Cloud gehostete Overlays haben Kunden zwei Optionen:

1. Überprüfen Sie, ob für Ihre Umgebung ein automatisches Upgrade geplant ist, indem Sie zu SSP > Overlay Details > Change Windows navigieren.
2. Wenn Sie nicht auf das geplante Upgrade warten möchten, haben Sie zwei Möglichkeiten:
    - Die in diesem Dokument verfügbaren Upgrade-Leitfäden unterstützen Sie dabei.
    - Öffnen Sie ein Standby-TAC-Ticket für Ihr bevorzugtes Wartungsfenster. Das TAC steht Ihnen bei Problemen mit dem Upgrade zur Verfügung.

F: Müssen auch die Edge-Router aktualisiert werden?

A : Nein, Cisco IOS XE-Geräte sind von dieser Ankündigung nicht betroffen.

Frage: Wir sind ein von Cisco gehostetes Overlay. Müssen ACLs behoben oder Maßnahmen für SSP ergriffen werden?

A : Allen von Cisco gehosteten Kunden wird empfohlen, ihre eigenen zulässigen eingehenden Regeln für SSP zu überprüfen und sicherzustellen, dass nur die von Ihnen benötigten Präfixe zulässig sind. Diese Regeln gelten nur für den Managementzugriff und nicht für Edge-Router. Überprüfen Sie diese unter SSP > Overlay Details > Allow Inbound rules (Eingehende Regeln zulassen). Beachten Sie, dass die Ports 22 und 830 bei der Bereitstellung durch Cisco von außen für die in der Cloud gehosteten Controller am Tag 0 standardmäßig immer blockiert wurden.

F: Wir befinden uns in der SD-WAN-Cloud (früher bekannt als Cloud Delivered Cisco Catalyst SD-WAN [CDCS]). Auf welche Version wird das Upgrade durchgeführt?

A : Basierend auf der aktuellen Version sind SD-WAN Cloud-Cluster aktuell im Zeitplan für ein Upgrade ODER bereits für ein Upgrade auf die festen Versionen. Hier sind die festen SD-WAN Cloud-Versionen (ehemals CDCS):

1. Early-Adopter-Cluster = 20.18.2.2 (entspricht der Standardversion)

2. Empfehlen Sie Release Cluster = 20.15.506 (CDCS-spezifische Version mit PSIRT Fixes)

SD-WAN-Cloud-Kunden müssen keine effektiven Maßnahmen ergreifen, um dieses PSIRT zu bewältigen.

F: Wir sind auf Shared Tenant. Auf welche Version wird das Upgrade durchgeführt?

A : Basierend auf der aktuellen Version ist für den Shared Tenant derzeit ein Upgrade geplant ODER bereits ein Upgrade auf die festen Versionen. Die Shared Tenant-Freigaben mit fester Konfiguration sind:

1. Empfohlene Release-Cluster = 20.15.5.2

F: Bietet das Cisco TAC forensische Analyse- oder Ermittlungsservices für diese Sicherheitslücken?

A : Das Cisco TAC kann Kunden bei der Suche nach Indicators of Compromise (IoCs) im Zusammenhang mit diesen Schwachstellen unterstützen. Das TAC führt jedoch keine detaillierte forensische Analyse oder Vorfalluntersuchungen durch. Für umfassende forensische Untersuchungen oder detaillierte Sicherheitsuntersuchungen empfehlen wir Kunden, sich an die von ihnen bevorzugte externe Incident Response (IR)-Firma zu wenden.

F: Welche allgemeinen Best Practices oder Möglichkeiten zur Reduzierung von Schwachstellen in meinem SD-WAN-Overlay gibt es?

A : Im Cisco Catalyst SD-WAN Hardening Guide (Leitfaden zur Absicherung von SD-WAN) finden Sie Best Practices und Empfehlungen zur Verringerung von Schwachstellen in Ihrem SD-WAN-Overlay.

F: Wir sehen Protokolle von einem "root"-Benutzer auf unserem System. Ist das Besorgnis

erregend?

A : Überprüfen Sie, was noch im System vor sich geht. Diese Protokolle können vollständig erwartet werden. Beispielsweise werden beim Generieren von admin-techs System-Login-Änderungsprotokolle eines "Root"-Benutzers angezeigt. Protokolle können auch von einem "Root"-Benutzer während eines Neustarts angezeigt werden.

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

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

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

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

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.