Sicherheitshinweis für Catalyst SD-WAN - Februar 2026

Inhalt

Einleitung

Voraussetzungen

- Anforderungen
- Verwendete Komponenten

Hintergrundinformationen

Behebungs-Workflow - Übersicht

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

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

Phase 2: TAC-Ticket öffnen und Admin-Tech-Dateien hochladen

Schritt 3: TAC-Analyse

Schritt 4: Problembehebung durchführen (TAC-orientiert)

- Pfad A: Keine Indications of Compromise gefunden - Upgrade
- Pfad B: Indications of Compromise identifiziert - PSIRT-geführt

Fest implementierte Softwareversionen

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

- Überprüfung 1: Suchen nach nicht autorisierten SSH-Anmeldungen in Auth-Protokollen
- Überprüfung 2: Suchen nach nicht autorisierten Peer-Verbindungen in Controller-Syslogs

Häufig gestellte Fragen

Einleitung

In diesem Dokument werden die Schritte zum Identifizieren und Beheben kritischer Sicherheitslücken in SD-WAN basierend auf PSIRT-Empfehlungen vom 25. Februar 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:

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

Diese Mängel werden durch folgende PSIRT-Ankündigungen behoben:

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

Behebungs-Workflow - Übersicht

Anmerkung: Alle SD-WAN-Bereitstellungen sind anfällig und erfordern sofortige Maßnahmen. Nicht alle Systeme weisen jedoch Anzeichen einer Kompromittierung auf.

Erforderliche Aktion: Öffnen Sie ein Cisco TAC-Ticket, um diese Sicherheitsempfehlung zu bearbeiten.

Das TAC ist verfügbar für:

- Bewertung der Umgebung auf Anzeichen für Kompromittierung
- Führen Sie den entsprechenden Behebungspfad basierend auf der Bewertung durch.
- Arbeiten Sie mit dem PSIRT-Team zusammen, wenn Anzeichen für eine Kompromittierung identifiziert werden.

- Beratung und Unterstützung bei Upgrades, wenn keine Anzeichen für Kompromittierung erkannt werden

1. Collect Admin-Techs: Führen Sie admin-tech für alle Steuerungskomponenten aus (vSmart, vManage, vBond). vSmart admin-techs darf nicht gleichzeitig ausgeführt werden, sondern muss einzeln ausgeführt werden. Alle anderen können in beliebiger Reihenfolge gesammelt werden. Wählen Sie die Optionen Protokoll und Technik aus. Core ist nicht erforderlich.
2. Open TAC Case - Kontaktieren Sie das Cisco TAC und stellen Sie alle Control Component Admin-Tech Log-Pakete bereit
3. TAC-Analyse - TAC bewertet Ihre Umgebung auf Anzeichen für Kompromittierung
4. Problembehebung durchführen - vom TAC bereitgestellter Prozess abschließen

---

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

Erforderlich: Sammeln Sie Admin-Tech-Dateien von allen Steuerungskomponenten, bevor Sie Ihr TAC-Ticket öffnen. Dies ist für das TAC zur Beurteilung Ihrer Umgebung unerlässlich.

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: TAC-Ticket öffnen und Admin-Tech-Dateien hochladen

Nachdem Sie alle Admin-Tech-Dateien aus Schritt 1 gesammelt haben, öffnen Sie ein Cisco TAC-Support-Ticket.

Erforderliche Aktionen:

1. Erstellen Sie ein TAC-Ticket mit dem Schweregrad, der Ihren geschäftlichen Auswirkungen entspricht.
2. Laden Sie ALLE in Schritt 1 gesammelten Admin-Tech-Protokollpakete hoch (Controller, Manager und Prüfer).
3. Verweisen auf die PSIRT-Ankündigungen
4. TAC-Analyse und Beratung abwarten

⚠ Vorsicht: Das TAC bestimmt den Status Ihres Systems und empfiehlt die nächsten Schritte.

Versuchen Sie keine weiteren Schritte ohne Anleitung durch das TAC.

Schritt 3: TAC-Analyse

Das TAC analysiert die hochgeladenen Admin-Tech-Dateien und ermittelt den Status Ihres Systems.

Während dieser Zeit:

- Abwarten einer offiziellen Bewertung durch das TAC, bevor Maßnahmen ergriffen werden
- TAC kontaktiert Sie mit seinen Ergebnissen und den nächsten Schritten

---

Schritt 4: Problembehebung durchführen (TAC-orientiert)

TAC führt Sie durch den entsprechenden Sanierungsprozess, basierend auf der Bewertung des Kunden. Befolgen Sie alle Anweisungen des TAC.

Pfad A: Keine Indications of Compromise gefunden - Upgrade

Wenn das TAC bestätigt, dass keine Anzeichen für eine Kompromittierung vorliegen, führen Sie ein Upgrade auf die feste Softwareversion durch. Wählen Sie aus der Tabelle Fixed Software Versions (Feste Softwareversionen) in diesem Dokument die entsprechende Version aus, und verweisen Sie auf den in diesem Abschnitt verknüpften Upgrade-Leitfaden.

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

Pfad B: Indications of Compromise identifiziert - PSIRT-geführt

Wenn das TAC bestätigt, dass Indicators of Compromise vorhanden sind, beauftragt es das PSIRT-Team, eine spezifische Sanierungsstrategie für Ihre Umgebung zu entwickeln. Befolgen Sie alle Vorgaben des TAC und des PSIRT.

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	20.9.8.2 *	20.9.8.2 Upgrade-Images für vManage, vSmart und vBond
20.10, 20.11, 20.12.5 und frühere Versionen in 20.12	20.12.5.3	20.12.5.3 Upgrade-Images für vManage, vSmart und vBond
20.12.6	20.12.6.1	20.12.6.1 Upgrade-Images für vManage, vSmart und vBond
20.13, 20.14, 20.15.x	20.15.4.2	20.15.4.2 Upgrade-Images für vManage, vSmart und vBond
20.16, 20.17, 20.18.x	20.18.2.1	20.18.2.1 Upgrade-Images für vManage, vSmart und vBond

Anmerkung: Für Kunden mit CDCS (Cisco-Hosted Cluster) ist 20.15.405 ebenfalls eine feste Version. Dies gilt speziell für die von Cisco gehostete Cluster-Bereitstellung und wird getrennt vom Standard-Upgrade-Pfad behandelt.

* Wenn Sie Version 20.9 oder älter sind: Die Software für Ihre Version (20.9.8.2) ist am 27.2.2 verfügbar. Cisco empfiehlt, innerhalb der aktuellen Hauptversion zu bleiben und auf die Version 20.9.8.2 zu warten, anstatt auf eine höhere Hauptversion (20.12, 20.15, 20.18) zu aktualisieren. Wenn Sie sich aktuell in einer Version unter 20.9 befinden, warten Sie, bis dort ein Upgrade auf 20.9.8.2 durchgeführt wird. Arbeiten Sie weiterhin mit dem TAC zusammen, und informieren Sie sich am 27.2. über den verfügbaren Software-Link.

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 den folgenden Befehl aus:

```
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
```

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

Häufig gestellte Fragen

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

Admin-Tech-Dateien von allen Steuerungskomponenten, und öffnen Sie ein TAC-Ticket, um die Dateien hochzuladen. Das TAC bewertet Ihre Umgebung und gibt Ihnen Hinweise zu den nächsten Schritten.

Frage: Auf welche Version sollte ich ein Upgrade durchführen? 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: Was passiert, wenn Anzeichen für eine Kompromittierung erkannt werden?

A : Das TAC holt das PSIRT-Team ein und setzt sich mit Ihnen in Verbindung, um die nächsten Schritte und die Anleitung speziell 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 : Nein, warten Sie, bis das TAC die Analyse abgeschlossen und sich beraten hat, bevor Sie Abhilfemaßnahmen ergreifen.

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: Sind die PSIRT-Korrekturen in der kommenden Version 20.15.5 und anderen kommenden Versionen enthalten?

A : Ja, Fixes sind in 20.15.5 und anderen kommenden Versionen enthalten. Das Upgrade zur Beseitigung der in diesem Dokument beschriebenen Schwachstellen muss jedoch SOFORT priorisiert werden. (Warten Sie nicht!)

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 hilft Ihnen bei Problemen mit dem Upgrade.

F: Müssen auch die Edge-Router aktualisiert werden?

A : 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 nutzen CDCS/Shared Tenant. Auf welche Version wird das Upgrade durchgeführt?

A : Basierend auf der aktuellen Version sind ein Upgrade der Shared Tenant- oder CDCS-Cluster derzeit geplant ODER ein Upgrade auf die festen Versionen ist bereits geplant. Die Shared Tenant- und CDCS Fixed-Versionen:

1. Early-Adopter-Cluster => 20.18.2.1 (entspricht der Standardversion)

2. Empfehlen Sie Release Cluster => 20.15.405 (CDCS-spezifische Version mit PSIRT Fixes)

CDCS-Kunden müssen keine wirksamen Maßnahmen ergreifen, um dieses PSIRT zu bewältigen.

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.

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.