

Remediate Catalyst SD-WAN Security Advisory - September 2026

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Behebungs-Workflow - Übersicht](#)

[Schritt 1: Admin-Tech-Dateien von allen Managern erfassen](#)

[Alternative: Manuelle Überprüfung \(nur wenn Admin-Tech nicht erfasst werden kann\)](#)

[Phase 2: Upgrade auf eine feste Softwareversion](#)

[Schritt 3: TAC-Ticket öffnen und Admin-Tech-Dateien zum Scannen hochladen](#)

[Schritt 4: Bei Identifizierung eines Kompromittierens - TAC-Richtlinien](#)

[Fest implementierte Softwareversionen](#)

[Anhang: Manuelle Verifizierungsschritte \(nur wenn Admin-Tech-Erfassung nicht möglich\)](#)

[Identifizierung von Indicators of Compromise](#)

[Überprüfung 1: Prüfen des Service-Proxy-Zugriffsprotokolls](#)

[Überprüfung 2: Manager-Serverprotokoll überwachen](#)

[Häufig gestellte Fragen](#)

Einleitung

In diesem Dokument werden die Schritte zum Identifizieren und Beheben einer kritischen SD-WAN-Sicherheitslücke gemäß den PSIRT-Gutachten vom 30. September 2026 beschrieben. Cisco empfiehlt dringend, zur Behebung dieses Problems ein Upgrade auf eine feste Softwareversion durchzuführen.

Voraussetzungen

Anforderungen

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

- Cisco Catalyst SD-WAN-Architektur und Steuerungskomponenten (Manager, Controller und Validator)
- 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 Ankündigung ist unter folgendem Link abrufbar:

- [Anfälligkeit für Cisco Catalyst SD-WAN Manager-API-Authentifizierung umgangen](#) (CVE-2026-76504, CWE-177). Bewertung der Sicherheitsauswirkungen: Kritisch (CVSS-Basisbewertung 9.8).

Dieser Mangel wird durch diese PSIRT-Beratung behoben:

- Cisco Bug-ID [CSCww79570](#)

Diese Ankündigung betrifft Cisco Catalyst SD-WAN Manager (vManage).

Behebungs-Workflow - Übersicht



Anmerkung: Alle SD-WAN-Manager (vManage), die eine frühere Version als die erste feste Version ausführen, sind anfällig und erfordern ein sofortiges Upgrade. Nicht alle Catalyst Manager sind jedoch in der Lage, eine Kompromittierung nachzuweisen.

Erforderliche Aktion: Sammeln Sie Admin-Techniker von allen Catalyst SD-WAN-Managern, aktualisieren Sie alle auf eine feste Version, und erstellen Sie ein Cisco TAC-Ticket, damit das TAC Ihre Admin-Techniker auf Anzeichen für eine Kompromittierung untersuchen 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. Admin-Tech sammeln: Führen Sie vor dem Upgrade admin-tech auf allen Catalyst SD-WAN-Managern aus, einschließlich aller Knoten eines Clusters und einer Disaster Recovery (DR)-Bereitstellung, um sicherzustellen, dass keine Diagnosedaten verloren gehen. Wählen Sie die Optionen Protokoll und Technik aus. Core ist nicht erforderlich.
2. Upgrade auf eine feste Version - Führen Sie für alle Manager (vManage) 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, verwenden Sie die TAC-Anleitung. Wenn das TAC Indicators of Compromise in Ihrer Umgebung identifiziert, füllen Sie alle vom TAC bereitgestellten Sanierungsleitfäden aus. Wenn keine Anzeichen für eine Kompromittierung gefunden werden, sind über das Upgrade hinaus keine weiteren Maßnahmen erforderlich.

Schritt 1: Admin-Tech-Dateien von allen Managern erfassen

Erforderlich: Sammeln Sie vor dem Upgrade Admin-Tech-Dateien von allen Managern (vManage), 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 Managern (vManage) aus.
2. Wenn Ihre Manager als Cluster ausgeführt werden, führen Sie admin-tech auf jedem Cluster-Mitglied aus.
3. Wenn Sie eine Disaster Recovery (DR)-Bereitstellung haben, führen Sie admin-tech auf jedem Manager sowohl am primären als auch am DR-Standort aus.

[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.

Ausführliche Informationen hierzu finden Sie im Abschnitt [Manuelle Korrekturschritte](#) 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 Admin-Techniker gesammelt haben, aktualisieren Sie alle Manager (vManage) 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 dem Schweregrad 3 und der CVE-ID "CVE-2026-76504" im Titel, um den Scanvorgang zu starten.
2. Laden Sie ALLE in Schritt 1 erfassten Admin-Tech-Protokollpakete hoch (alle Manager, einschließlich Cluster- und DR-Knoten).
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 Identifizierung eines Kompromittierens - TAC-Richtlinien

Wenn das TAC Anzeichen für eine Kompromittierung in Ihrer Umgebung identifiziert, setzt sich das TAC mit Ihnen in Verbindung und hilft Ihnen bei der Problembeseitigung. 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 die Behebung dieser Schwachstelle. Aktualisieren Sie auf die erste feste Version in Ihrem aktuellen Release Train.

Cisco Catalyst SD-WAN-Softwareversion	Erste feste Version	Verfügbare Software
Früher als 20.9 ¹	Migrieren Sie zu einer festen Version.	
20.9	20.9.10.1	20.9.10.1 Upgrade-Images für vManage

Cisco Catalyst SD-WAN-Softwareversion	Erste feste Version	Verfügbare Software
20.12	20.12.8.2	20.12.8.2 Upgrade-Images für vManage
20.15	20.15.6.1	20.15.6.1 Upgrade-Images für vManage
20.18	20.18.4.1	20.18.4.1 Upgrade-Images für vManage
26.1	26.1.2.1	26.1.2.1 Upgrade-Images für vManage
26.2	26.2.1	26.2.1 Upgrade-Images für vManage

¹ Diese Versionen haben das Ende der Softwarewartung erreicht. Cisco empfiehlt Kunden dringend, ein Upgrade auf eine unterstützte Version durchzuführen.

Das Cisco Product Security Incident Response Team (PSIRT) validiert nur die betroffenen und festen Versionsinformationen, die im Advisory dokumentiert sind.



Anmerkung: Cisco hat diese Schwachstelle auch in der Cloud-basierten Version 20.15.605 des Cisco SD-WAN Cloud (Cisco Managed) behoben. Es ist keine Benutzeraktion erforderlich. Kunden können den aktuellen Behebungsstatus oder die aktuelle Softwareversion über die Hilfe-Funktion in der Service-GUI ermitteln.

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 auf allen Managern (vManage) ausgeführt werden, einschließlich aller Cluster-Mitglieder und aller Manager an einem Disaster Recovery-Standort (DR). Greifen Sie auf die Protokolldateien von vshell (vshell von der Manager-CLI) zu, und überprüfen Sie sowohl die aktuellen als auch die rotierten Protokolldateien.

Identifizierung von Indicators of Compromise

Dieses Gutachten weist zwei Kompromissindikatoren auf. Beide beziehen sich auf Einträge für j_security_check, in denen ein Zeichen der Anforderung codiert ist (z.B. /%6a_security_check), von unbekannten oder nicht autorisierten IP-Adressen.



Wichtig: Die Beispiele in diesem Abschnitt zeigen die Verwendung von %6a als codiertes Zeichen j in der Anforderung. Dies ist nur ein Beispiel, und die Schwachstelle ermöglicht die Verwendung eines beliebigen Zeichens, das in der Anfrage codiert ist.



Anmerkung: Bei Cisco Catalyst SD-WAN Manager-Systemen, die mit dem Internet verbunden sind und über Anschlüsse verfügen, die mit dem Internet verbunden sind, besteht das Risiko einer Gefährdung. In einigen Fällen können diese Anzeichen für eine Kompromittierung bei Standardvorgängen auftreten. Daher müssen sie im Vergleich zum normalen Netzwerkstatus bewertet werden, um Fehlalarme zu identifizieren und zu vermeiden.

Anzeige	Protokolldatei	Bedeutung	V
Codierte j_security_check-Anforderung empfangen	/var/log/nms/containers/service_proxy/serviceproxy-access.log*	Ein Client hat eine Anforderung dieses Typs an den Manager gesendet.	Ü 1

Anzeige	Protokolldatei	Bedeutung	V
Codierte j_security_check- Anfrage für einen viptela- reservierten-* Benutzer verarbeitet	/var/log/nms/vmanage-server.log*	Der Manager hat eine solche Anforderung für einen viptela- reservierten-* Benutzer (ein reserviertes Systemdienstkonto) bearbeitet.	Ü 2

Überprüfung 1: Prüfen des Service-Proxy-Zugriffsprotokolls

Überprüfen Sie die Datei `serviceproxy-access.log` unter `/var/log/nms/containers/service_proxy/serviceproxy-access.log` auf Einträge, die sich auf `j_security_check` beziehen, von unbekannten oder nicht autorisierten IP-Adressen, wie in diesem Beispiel gezeigt:

```
[2026-09-29T23:11:13.948-05:00] "POST /%6a_security_check HTTP/1.1" 200 - 48 0 4 - "10.10.10.47,192.168
```

Bestimmte Protokolldateien im vManage-System sind auf Root-Zugriff beschränkt und können von Kunden nicht direkt aufgerufen werden. Um diese Protokolle überprüfen zu können, müssen Kunden eine Admin-Tech-Datei erstellen.

Interpretation der Ergebnisse und Dokumentation für das TAC

Wenn keine solchen Einträge gefunden werden:

- In diesem Protokoll auf diesem Manager wurden keine Anzeichen für eine Kompromittierung erkannt.
- Dokumentieren Sie dieses Ergebnis für Ihren TAC-Ticket.
- Fahren Sie mit Überprüfung 2 fort, und wiederholen Sie dann beide Überprüfungen für die verbleibenden Manager.

Wenn solche Einträge gefunden werden:

- Überprüfen Sie sorgfältig alle angezeigten Quell-IP-Adressen.
- Suchen Sie nach Einträgen von unbekannten oder nicht autorisierten IP-Adressen. Überprüfen Sie, ob die Quell-IP zu einer autorisierten Aktivität in Ihrer Umgebung gehört (z. B. eine Suche nach Schwachstellen oder ein Penetrationstest, den Sie ausführen).
- 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.
- Schließen Sie Protokolleinträge, Zeitstempel, Quell-IPs und HTTP-Statuscodes in Ihr Gehäuse ein.

- TAC führt offizielle Bewertungsbestimmung durch

Überprüfung 2: Manager-Serverprotokoll überwachen

Überprüfen Sie die Datei `vmanage-server.log` unter `/var/log/nms/vmanage-server.log` auf Einträge, die sich auf `j_security_check` beziehen, und zwar von unbekannten oder nicht autorisierten IP-Adressen, die speziell für Benutzer aufgerufen werden, die Namen enthalten, die mit `viptela-reserved-` beginnen, wie in diesem Beispiel gezeigt:

```
29-Sep-2026 23:11:13,952 CDT [] [vManage-new] [UserUtils] (default task-127462) |default| Request Store
```



Anmerkung: Die `viptela-reservierten` System-Service-Konten werden im Abschnitt Authentifizierung, Autorisierung und Abrechnung des Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide dokumentiert.

Interpretation der Ergebnisse und Dokumentation für das TAC

Wenn keine solchen Einträge gefunden werden:

- In diesem Protokoll auf diesem Manager wurden keine Anzeichen für eine Kompromittierung erkannt.
- Dokumentieren Sie dieses Ergebnis für Ihren TAC-Ticket.
- Wiederholen Sie beide Überprüfungen für die verbleibenden Manager.

Wenn solche Einträge gefunden werden:

- Dies kann potenzielle Anzeichen für eine Kompromittierung anzeigen.
- Dokumentieren Sie alle Ergebnisse, und eröffnen Sie sofort ein TAC-Ticket.
- Fügen Sie die Protokolleinträge und Zeitstempel in Ihrem Fall hinzu, zusammen mit den Ergebnissen von Verification 1 für denselben Zeitraum.
- 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 Managern (vManage) und aktualisieren Sie dann alle Manager 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.

F: Welche Komponenten sind von dieser Beratung betroffen?

A : Nur Cisco Catalyst SD-WAN Manager (vManage) ist betroffen.

F: Müssen wir auch die Controller, Validatoren oder Edge-Router aktualisieren?

A : Nein, ich möchte mich nicht an diesen Hinweis wenden. Führen Sie für alle Manager (vManage) ein Upgrade auf eine feste Version durch, und verwenden Sie die [Controller-Kompatibilitätsmatrix](#), um sicherzustellen, dass die neue Manager-Version mit Ihren anderen Komponenten kompatibel ist.

F: Gibt es eine Problemumgehung?

A : Nein. Es gibt keine Problemumgehungen, die diese Schwachstelle beheben. Upgrade auf eine feste Version

F: Auf welche Version muss ich ein Upgrade durchführen?

A : Upgrade auf die erste feste Version in Ihrem aktuellen Release-Zug so schnell wie möglich. Weitere Informationen finden Sie in der Tabelle [Fixed Software](#) Versions in diesem Dokument. TAC bestätigt die für Ihre spezifische Umgebung passende Version.

F: Ich habe bereits ein Upgrade auf eine feste Version für eine vorherige SD-WAN-Sicherheitsempfehlung durchgeführt. Muss ich das Upgrade erneut durchführen?

A : Ja, es sei denn, Ihre aktuelle Version ist auf oder später als die erste feste Version in Ihrem Zug in der Tabelle [feste Softwareversionen](#). Behobene Versionen für frühere Ankündigungen beinhalten nicht unbedingt die Behebung dieser Schwachstelle.

F: Muss ich Admin-Techniker von allen Managern abholen?

A : Ja. Das TAC erfordert Admin-Tech-Dateien von jedem Manager (vManage), einschließlich jedem Cluster-Mitglied und jedem Manager an einem Disaster Recovery-Standort (DR), um Ihre Umgebung richtig zu bewerten.

F: Kann ich selbst nach Anzeichen für eine Kompromittierung suchen?

A : Ja. Wenn Sie keine Admin-Tech-Dateien sammeln können, verwenden Sie die [manuellen Überprüfungsschritte](#) auf jedem Manager, und geben Sie die Ergebnisse an das TAC weiter. Die Erfassung durch die Admin-Technik bleibt die bevorzugte Methode, und das TAC trifft die offizielle Bewertungsentscheidung.

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 : 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: 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: 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: Wir sind ein von Cisco gehostetes Overlay. Müssen wir die Zugangsregeln für die SSP überprüfen?

A : Allen von Cisco gehosteten Kunden wird empfohlen, ihre eigenen zulässigen eingehenden Regeln unter SSP > Overlay-Details > Eingehende Regeln zulassen zu überprüfen und sicherzustellen, dass nur die erforderlichen Präfixe von Ihrer Seite zugelassen werden. Diese Regeln gelten nur für den Managementzugriff und nicht für Edge-Router.

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

A : Das Cisco TAC kann Kunden bei der Suche nach Indicators of Compromise (IoCs) im Zusammenhang mit dieser Schwachstelle 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.

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.