Remediate Catalyst SD-WAN Security Advisory - Juni 2026

Inhalt

Einleitung

In diesem Dokument werden die Schritte zur Identifizierung und Behebung kritischer Sicherheitslücken im SD-WAN auf der Grundlage der PSIRT-Empfehlungen vom 4. Juni 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:

- Anfälligkeit für authentifizierte Rechteausweitung durch Cisco Catalyst SD-WAN Manager

Diese Mängel werden durch folgende PSIRT-Ankündigungen behoben:

- Cisco Bug-ID CSCwu18563

Behebungs-Workflow - Übersicht

Diese Ankündigung beschreibt eine Schwachstelle bei der Rechteausweitung im SD-WAN-Manager, die zur Ausnutzung von Rechten des Netzwerkadministrators erforderlich ist.

Laut der Ankündigung sind die bekannten Pfade, über die ein nicht authentifizierter Remote-Angreifer diese Privilegien erlangen kann, die Ausnutzung von CVE-2026-20182 (cisco-sa-sdwan-rpa2-v69WY2SW) oder CVE-2026-20127 (cisco-sa-sdwan-rpa-EHchtZk).

Wenn Ihre Steuerungskomponenten für beide Ankündigungen auf eine feste Version aktualisiert wurden und Cisco keine potenziellen Indicators of Compromise (IoCs) in den Admin-Tech-Dateien identifiziert hat, die Sie für die vorherigen Ankündigungen bereitgestellt haben, werden die bekannten nicht authentifizierten Exploit-Pfade für diese neue Schwachstelle auf diesen spezifischen Geräten anhand der überprüften Dateien minimiert.

Dies schließt die Offenlegung nicht aus, wenn ein Angreifer gültige Netadmin-Anmeldeinformationen besitzt. Cisco hat für diese Schwachstelle noch keinen Software-Fix herausgegeben, und es sind keine Problemumgehungen verfügbar. Weitere Leitlinien werden folgen, sobald sie vorliegen.

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.
- Bereitstellung von Leitlinien für die nächsten Schritte, die bei der Ermittlung von Indicators of Compromise erforderlich sind

1. Sammeln von Admin-Tech- 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. TAC-Ticket öffnen - Wenden Sie sich an das Cisco TAC, und stellen Sie alle Admin-Tech-Protokollpakete für Steuerungskomponenten zur Verfügung.
3. TAC-Bewertung: Führen Sie eine vorläufige Bewertung der Indications of Compromise in Ihrer Umgebung durch, und das TAC führt eine vorläufige Bewertung der Indications of Compromise in Ihrer Umgebung durch.
4. Durchführung der Problembehebung: Führen Sie ggf. den vom TAC bereitgestellten spezifischen Prozess aus.

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

Erforderlich: Erfassen Sie vor Upgrades oder Konfigurationsänderungen Admin-Tech-Dateien von allen Steuerungskomponenten, sodass Diagnosedaten und potenzielle Indications of Compromise (IoCs) erhalten bleiben. Diese Dateien werden vom TAC in Schritt 3 verwendet, um Ihre Umgebung zu analysieren.

Sammlung: Wählen Sie für die Administrator-Tech-Generation die Optionen Log und Tech aus. 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

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 im Zusammenhang mit dieser Ankündigung hin zu prüfen. Die Analyse für diese Ankündigung konzentriert sich auf einen spezifischen Protokolleintrag, der nicht zwischen legitimer und böswilliger Verwendung unterscheidet. eine manuelle Überprüfung durch das TAC erforderlich ist.

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

Für Kunden, die keine Admin-Tech-Dateien freigeben können, steht ein manueller Verifizierungsschritt zur Verfügung. Dieser Schritt enthält einen vorläufigen Indikator, der dokumentiert und an das TAC weitergegeben werden muss.

Ausführliche Informationen 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

Nach dem Sammeln der Admin-Techniker in Schritt 1 öffnen Sie ein Cisco TAC-Support-Ticket und laden die gesammelten Admin-Tech-Dateien hoch. Das TAC analysiert die Admin-Techniker auf Indications of Compromise, die mit diesem Advisory verbunden sind.

Erforderliche Aktionen:

1. Öffnen Sie ein TAC-Ticket mit Schweregrad 3 mit "CVE-2026-20245" und der Beratungs-ID `cisco-sa-sdwan-privesc-4uxFrdzx` im Titel, um die Analyse zu initiieren.
2. Laden Sie ALLE in Schritt 1 gesammelten Admin-Tech-Protokollpakete hoch (Controller, Manager und Prüfer).
3. Warten Sie, bis das TAC die Analyse abgeschlossen und die Ergebnisse kommuniziert hat.

Anmerkung: Cisco hat keinen Software-Fix für diese Schwachstelle veröffentlicht, und es sind keine Problemlösungen verfügbar. Anhand der TAC-Analyse in Schritt 3 kann festgestellt werden, ob in den von Ihnen bereitgestellten Admin-Tech-Dateien Anzeichen für eine Kompromittierung vorhanden sind. Weitere Anleitungen werden folgen, sobald sie von den Technikern zur Verfügung gestellt werden.

Schritt 3: TAC-Analyse

Das TAC führt eine vorläufige Analyse der Admin-Tech-Dateien durch, die Sie in Schritt 2 hochgeladen haben, und bewertet sie auf Anzeichen für eine Kompromittierung im Zusammenhang mit diesem Gutachten.

Bei dieser Ankündigung konzentriert sich die Analyse auf einen bestimmten Protokolleintrag in `/var/log/scripts.log` für jeden Manager (vManage). Da der zugrunde liegende Befehl legitim ist und das Protokoll nicht zwischen legitimer und böswilliger Verwendung unterscheidet, müssen alle übereinstimmenden Einträge manuell vom TAC auf den normalen Betriebsstatus des Kunden überprüft werden, bevor sie als bestätigter Indikator behandelt werden.

Mögliche Ergebnisse der TAC-Analyse:

- Keine übereinstimmenden Protokolleinträge identifiziert — basierend auf den überprüften admin-tech-Dateien wurden keine Indikatoren beobachtet, die mit dieser Meldung in Verbindung standen. Derzeit sind keine weiteren Maßnahmen speziell für diese Ankündigung erforderlich. Das Ergebnis ist auf die empfangenen Admin-Tech-Dateien beschränkt und kann durch die Protokollaufbewahrungszeit auf jedem Gerät begrenzt werden.
- Übereinstimmende Protokolleinträge identifiziert - TAC wendet sich an den Kunden mit zusätzlichen Überprüfungsschritten. Da Cisco für diese Ankündigung keinen Software-Fix veröffentlicht hat, kann diese Schwachstelle durch das Upgrade allein nicht behoben werden. Die TAC-Richtlinien für bestätigte Kompromittierungsszenarien werden in den entsprechenden TechZone-Artikeln dokumentiert, auf die in Schritt 4 verwiesen wird.

Anmerkung: Laut der Ankündigung erfordert die Ausnutzung dieser Verwundbarkeit netadmin-Privilegien, die ein nicht authentifizierter Angreifer nur durch gültige Anmeldeinformationen oder die Ausnutzung von CVE-2026-20182 oder CVE-2026-20127 erhalten kann. Wenn Ihre Kontrollkomponenten für beide Ankündigungen auf eine feste Version aktualisiert wurden und keine Anzeichen für eine Kompromittierung für die vorherigen Ereignisse identifiziert wurden, wurden die bekannten nicht authentifizierten Ausnutzungspfade für diese neue Schwachstelle werden auf diesen spezifischen Geräten mithilfe der überprüften Dateien gemindert.

Schritt 4: Wenn Anzeichen für eine Kompromittierung erkannt werden - Befolgen Sie die TAC-Richtlinien

Wenn das TAC Indicators of Compromise identifiziert, die mit diesem Gutachten in Ihrer Umgebung in Verbindung stehen, setzt sich das TAC mit Ihnen in Verbindung. Befolgen Sie alle Anweisungen des TAC.

Wenn keine Anzeichen für eine Kompromittierung für dieses Gutachten festgestellt werden, sind derzeit keine weiteren speziell auf dieses Gutachten bezogenen Maßnahmen erforderlich, die auf den überprüften Admin-Tech-Dateien basieren.

Wichtig: Cisco hat für diese Ankündigung keinen Software-Fix veröffentlicht, und es sind keine Problemumgehungen verfügbar. Da die Ausnutzung dieser Schwachstelle Netadmin-Berechtigungen erfordert, die über CVE-2026-20182 oder CVE-2026-20127 erlangt wurden, sollten Kunden sicherstellen, dass die Beseitigung dieser vorherigen Ankündigungen abgeschlossen ist. Weitere Informationen zu den ermittelten Abhilfemaßnahmen finden Sie in den entsprechenden Dokumenten:

Überlegungen

Nach Abschluss einer erfolgreichen Sanierung und auf der Grundlage der spezifischen Sicherheitsanforderungen des jeweiligen Kunden möchten die Kunden möglicherweise die folgenden Hygienemaßnahmen evaluieren und darauf reagieren. Diese Aktivitäten gelten unabhängig von der gewählten Behebungsoption. Sie werden vom Kunden verwaltet. Cisco leitet oder führt diese nicht im Namen des Kunden durch.

- Überprüfung aller lokalen Benutzerkonten
- Rotation der Mandate
- Rotation von eventuell vorhandenen Geheimnissen in Gerätekonfigurationen, z. B. (nicht erschöpfende Liste):
    - Anmeldeinformationen für lokale Benutzerkonten
    - SNMP-Gemeinschaftszeichenketten
    - TACACS - geheime Schlüssel
    - VPN Pre-Shared Keys und Zertifikate
    - Vertrauenswürdige SSH-Schlüssel
- Überprüfen von Konfigurationsvorlagen

Edge-Geräte - Verdächtige Kompromittierung

Cisco empfiehlt keinen bestimmten Wiederherstellungspfad. die Auswahl einer Sanierungsoption liegt beim Kunden. Zur Information für Kunden, die ihre Umgebung evaluieren: Wenn der Kunde eine Kompromittierung eines Edge-Geräts vermutet, handelt es sich bei einem Zurücksetzen auf die Werkseinstellungen und dem erneuten Onboarding der betroffenen Edge-Geräte um eine vom Kunden verwaltete Aktion, die der Kunde bei der Auswahl berücksichtigen möchte. Die Entscheidung, ob und welche Option Sie wählen, liegt beim Kunden.

Der richtige Befehl zum Durchführen eines sicheren Zurücksetzens auf die Werkseinstellungen lautet:

```
factory-reset all secure 3-pass
```

Fest implementierte Softwareversionen

⚠ Wichtig: Zum Zeitpunkt der Veröffentlichung dieses Dokuments hat Cisco noch keinen Software-Fix zur Behebung des Problems CVE-2026-20245 veröffentlicht. Laut der Ankündigung plant Cisco, diese Schwachstelle im Cisco Catalyst SD-WAN Manager in einer zukünftigen Version zu beheben. Es gibt keine Problemumgehungen. Dieser Abschnitt wird aktualisiert, sobald feste Software verfügbar ist.

Da die Ausnutzung dieser Schwachstelle Netadmin-Berechtigungen erfordert, die ein nicht authentifizierter Angreifer nur über CVE-2026-20182 oder CVE-2026-20127 erhalten kann, sollten Kunden sicherstellen, dass ihre Kontrollkomponenten eine feste Version für diese früheren Ankündigungen ausführen. Die festgelegten Versionen für diese Ratgeber sind im SD-WAN Security Advisory vom 14. Mai 2026 und im entsprechenden TechZone-Dokument dokumentiert:

- Sicherheitslücke bei Authentifizierung des Cisco Catalyst SD-WAN-Controllers umgangen (14. Mai 2026)
- (Tabelle der festen Softwareversionen)

Wichtige Hinweise:

- Upgrade-Matrix
- Controller-Kompatibilitätsmatrix

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

Anmerkung: Admin-Tech Collection ist die bevorzugte Methode. Verwenden Sie den unten stehenden manuellen Verifizierungsschritt nur, wenn Admin-Tech-Dateien nicht gesammelt und mit dem TAC gemeinsam genutzt werden können. Das Ergebnis dieses manuellen Schrittes ist vorläufig. die Ergebnisse zu dokumentieren und sie mit dem TAC zu teilen, der die offizielle Bewertung durchführt.

Anmerkung: Bei dieser Ankündigung besteht die manuelle Überprüfung aus einer einzigen gezielten Protokollprüfung. Der gesuchte Protokolleintrag wird durch einen legitimen Befehl generiert, und das Protokoll allein unterscheidet nicht zwischen legitimer und böswilliger Verwendung. Alle übereinstimmenden Einträge müssen mit dem normalen Betriebsstatus des Kunden abgeglichen werden, bevor sie als potenzieller Indikator behandelt werden. Wenn ein übereinstimmender Eintrag nicht mit dem normalen Betrieb abgeglichen werden kann, dokumentieren Sie das Ergebnis, und geben Sie es dem TAC weiter.

Überprüfen: Suchen Sie in `scripts.log` nach Einträgen zum Hochladen der Tenant-Liste in jedem Manager (vManage).

Gemäß der PSIRT-Ankündigung wird Kunden empfohlen, die Datei `scripts.log` unter /`var/log/` auf Einträge zu überprüfen, die dem folgenden Beispiel ähneln:

```
Apr 15 09:44:57 vmanage vScript: Tenant list upload per vsmart serial number: /usr/bin/vconfd_script_up
```

Schritt 1: Rufen Sie vshell auf jedem Manager (vManage) auf, und durchsuchen Sie die Protokolldatei.

Wechseln Sie von der vManage-CLI in vshell, und führen Sie Folgendes aus:

```
vs
zgrep "vconfd_script_upload_tenant_list.sh" /var/log/scripts.log*
```

Wiederholen Sie die Prüfung für alle vManage in der Bereitstellung (einschließlich aller Cluster-Mitglieder und aller DR-gepaarten vManage).

Phase 2: Interpretation der Ergebnisse und Dokumentation für das TAC

Wenn KEINE übereinstimmenden Einträge zurückgegeben werden:

- In der Protokolldatei auf diesem Gerät wurden keine Anzeichen für eine Kompromittierung im Zusammenhang mit dieser Meldung festgestellt.
- Dokumentieren Sie dieses Ergebnis für Ihren TAC-Fall (geben Sie den Hostnamen des Geräts und das Datum/den Bereich der durchsuchten Protokolldateien an).
- Überprüfen Sie weiterhin die verbleibenden Manager.

Wenn übereinstimmende Einträge zurückgegeben werden:

- Jeder übereinstimmende Eintrag muss anhand des normalen Betriebsstatus des Kunden überprüft werden. Der zugrunde liegende Befehl (Hochladen der Tenant-Liste) ist legitim und kann bei Routinevorgängen angezeigt werden.
- Erfassen Sie für jeden passenden Eintrag den Zeitstempel, die vollständige Protokollzeile und den Dateipfad, auf den nach dem `-CLI-Pfad` verwiesen wird.
- Wenn ein übereinstimmender Eintrag nicht mit einem bekannten, legitimen Vorgang abgeglichen werden kann, kann dies ein Anzeichen für eine Kompromittierung sein. Dokumentieren Sie die Ergebnisse, und stellen Sie sie dem TAC zur Überprüfung zur Verfügung.
- Dokumentieren Sie alle Ergebnisse, und öffnen Sie ein TAC-Ticket. Schließen Sie die übereinstimmenden Protokolleinträge und die Ausgabe des Quellbefehls in Ihren Fall ein.
- Das TAC führt die offizielle Bewertung durch. Wenn bei der Bewertung Anzeichen für eine Kompromittierung festgestellt werden, folgen Sie den Anweisungen in den entsprechenden TechZone-Dokumenten: und Sanierungsleitfäden.

Häufig gestellte Fragen

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

A : Sammeln Sie vor Upgrades oder Konfigurationsänderungen Admin-Tech-Dateien von allen Steuerungskomponenten (vSmart, vManage, vBond), um Diagnosedaten und potenzielle Indications of Compromise beizubehalten. Öffnen Sie dann ein Cisco TAC-Ticket, und laden Sie die Admin-Techniker hoch, damit das TAC sie analysieren kann.

F: Hat Cisco einen Software-Fix für diese Schwachstelle veröffentlicht?

A : Nicht zum Zeitpunkt der Veröffentlichung dieses Dokuments. Entsprechend der Ankündigung plant Cisco, diese Schwachstelle im Cisco Catalyst SD-WAN Manager in einer zukünftigen Version zu beheben. Es gibt keine Problemumgehungen. Dieses Dokument wird aktualisiert, sobald eine feste Version verfügbar ist.

F: Wenn es keine Lösung gibt, warum empfiehlt Cisco, jetzt etwas zu unternehmen?

A : Die Ausnutzung dieser Schwachstelle erfordert Netadmin-Berechtigungen. Ein nicht authentifizierter Angreifer kann diese Privilegien nur durch gültige Anmeldeinformationen oder durch die Ausnutzung von CVE-2026-20182 oder CVE-2026-20127 erlangen. Durch das Sicherstellen, dass Steuerungskomponenten auf die festen Versionen für diese vorherigen Advisories aktualisiert werden, werden die bekannten nicht authentifizierten Pfade adressiert, um die Privilegien zu erhalten, die erforderlich sind, um diese Schwachstelle auszunutzen. Anhand der admin-tech-Analyse in Schritt 3 kann festgestellt werden, ob in den überprüften Dateien Anzeichen für eine Kompromittierung vorhanden sind.

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

A : Ja. Das TAC benötigt Admin-Tech-Dateien von allen Controllern (vSmart, jeweils eine erfasst), allen Managern (vManage) und allen Validatoren (vBond), um die Analyse durchzuführen.

F: Wie ermittelt das TAC, ob mit diesem Gutachten Indications of Compromise für mein System verbunden sind?

A : Das TAC überprüft die Admin-Tech-Dateien und sucht auf jedem Manager nach dem spezifischen Protokolleintrag, der in der PSIRT-Ankündigung in `/var/log/scripts.log` beschrieben ist. Der zugrunde liegende Befehl ist legitim. Alle übereinstimmenden Einträge müssen mit dem normalen Betriebsstatus abgeglichen werden, bevor sie als potenzieller Indikator behandelt werden. TAC führt diese Prüfung durch.

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

A : TAC setzt sich mit Ihnen in Verbindung. Da für diese Ankündigung derzeit kein Software-Fix verfügbar ist, wird eine bestätigte Kompromittierung durch das Upgrade allein nicht behoben. Die Anleitung des TAC folgt den in den entsprechenden TechZone-Artikeln für die Ratschläge vom Mai 2026 und Februar 2026 dokumentierten Fluss.

F: Sind Edge-Router (Cisco IOS XE) von dieser Beratung betroffen?

A : Diese Ankündigung betrifft den Cisco Catalyst SD-WAN Manager. Cisco konnte laut der Ankündigung in begrenzten Fällen beobachten, dass die Ausnutzung dieser Schwachstelle zu einer Konfigurationsänderung führte, die an die Edge-Geräte weitergegeben wurde. Kunden wird

empfohlen, die Konfiguration ihrer Edge-Geräte zu überprüfen.

F: Welche Bereitstellungsarten sind betroffen?

A : Laut der Ankündigung betrifft diese Schwachstelle alle Bereitstellungsarten von Cisco Catalyst SD-WAN Manager, unabhängig von der Gerätekonfiguration, einschließlich Bereitstellung am Standort, Cisco SD-WAN Cloud-Pro, Cisco SD-WAN Cloud (Cisco Managed) und Cisco SD-WAN for Government (FedRAMP).

F: Ich habe die Ankündigungen für Mai 2026 und Februar 2026 bereits aktualisiert, und es wurden keine Anzeichen für eine Kompromittierung für diese Ereignisse ermittelt. Bin ich dieser neuen Verwundbarkeit ausgesetzt?

A : Wenn Ihre Kontrollkomponenten eine feste Version sowohl für CVE-2026-20182 als auch für CVE-2026-20127 ausführen und keine Anzeichen für eine Kompromittierung für diese vorherigen Ereignisse in den überprüften Admin-Tech-Dateien identifiziert wurden, werden die bekannten nicht authentifizierten Exploit-Pfade für diese neue Schwachstelle auf diesen spezifischen Geräten, basierend auf den überprüften Dateien, gemindert. Dies schließt die Offenlegung nicht aus, wenn ein Angreifer gültige NetAdmin-Anmeldeinformationen besitzt.

F: Kann ich die Überprüfung selbst durchführen, anstatt auf das TAC zu warten?

A : Kunden, die keine Admin-Techniker gemeinsam nutzen können, können den im Anhang beschriebenen manuellen Verifizierungsschritt durchführen. Das Ergebnis ist vorläufig. die Ergebnisse zu dokumentieren und sie mit dem TAC zu teilen, der die offizielle Bewertung durchführt.

F: Welche allgemeinen Best Practices gelten für die Härtung meines SD-WAN-Overlays?

A : Best Practices finden Sie im Cisco Catalyst SD-WAN Hardening Guide.

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

A : Das Cisco TAC kann Kunden helfen, indem es Admin-Tech-Dateien auf die Indications of Compromise überprüft, die im PSIRT-Gutachten dokumentiert sind. Das Cisco TAC führt keine umfassenden forensischen Analysen oder Vorfalluntersuchungen durch. Für umfassende forensische Arbeiten oder detaillierte Sicherheitsuntersuchungen wird empfohlen, dass die Kunden sich an ihre bevorzugte externe Incident Response (IR)-Firma wenden.

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.