

# Überprüfen Sie das SD-WAN PSIRT mit dem Tool zur Fehlerüberprüfung.

## Inhalt

---

[Einleitung](#)

[Anforderungen](#)

[Admin-Tech-Erzeugungsrichtlinien](#)

[Einschränkungen](#)

[Auslastung](#)

[Überprüfung einer Admin-Tech](#)

[Ergebnisse - Keine Indikatoren](#)

[Ergebnisse - gefundene Indikatoren](#)

[Analyse einer zusätzlichen Admin-Tech](#)

[Zusätzliche Optionen](#)

---

## Einleitung

In diesem Dokument wird die Verwendung des Bug-Anwendungs-Tools zum Scannen von Admin-Tech-Dateien nach möglichen Indicators of Compromise (IoCs) im Zusammenhang mit dem SD-WAN Product Security Incident Response Team (PSIRT) CVE-2026-20182 [CSCwt50498](#) [beschrieben](#).

## Anforderungen

Für [CSCwt50498](#) müssen Sie eine Admin-Tech Ihrer SD-WAN-Steuerungskomponenten generieren. Die Admin-Technik für den Controller (vSmart) muss einzeln generiert werden.

Die Admin-Technik anderer SD-WAN-Steuerungskomponenten kann in beliebiger Reihenfolge generiert werden.

## Admin-Tech-Erzeugungsrichtlinien

Wenn Sie Hilfe beim Erstellen dieser Dateien benötigen, lesen Sie dieses Dokument, in dem die Schritte zum Generieren eines Admin-Tech beschrieben werden: [So erfassen Sie eine Admin-](#)

## Einschränkungen

- Die Dateigröße ist derzeit auf 500 MB beschränkt.
- Eine gleichzeitige Dateiüberprüfung wird nicht unterstützt. Das Tool kann mehrere Dateien verarbeiten, aber jeweils nur eine.

## Auslastung

### Überprüfung einer Admin-Tech

1. Rufen Sie das Cisco Bug Search Tool auf, um die Cisco Bug-ID zu erhalten, die Sie analysieren möchten.
2. Klicken Sie unter dem Titel auf den Text oder das Symbol "Check Bug Applicability". Ein Popup-Fenster wird angezeigt.
3. Löschen oder wählen Sie die Admin-Tech-Datei, die Sie analysieren möchten.

## Bug Search Tool

### Cisco Catalyst SD-WAN Controller Authentication Bypass Vulnerability

CSCwt50498 | [Check Bug Applicability](#)

[Customer Visible](#) [Notifications](#) [Save Bug](#) [Open Support Case](#)

#### Description

**Symptom:**

May 2026: This security advisory provides the details and fix information for a vulnerability that was discovered and fixed after the Cisco Catalyst SD-WAN Controller Authentication Bypass Vulnerability was disclosed in February 2026. This new advisory is for a new vulnerability in the control connection handshaking. The Indicators of Compromise section of this advisory includes Show Control Connections guidance to help with system checks.

A vulnerability in the peering authentication in Cisco Catalyst SD-WAN Controller, formerly SD-WAN vSmart, and Cisco Catalyst SD-WAN Manager, formerly SD-WAN vManage, could allow an unauthenticated, remote attacker to bypass authentication and obtain administrative privileges on an affected system.

This vulnerability exists because the peering authentication mechanism in an affected system is not working properly. An attacker could exploit this vulnerability by sending crafted requests to the affected system. A successful exploit could allow the attacker to log in to an affected Cisco Catalyst SD-WAN Controller as an internal, high-privileged, non-root user account. Using this account, the attacker could access NETCONF, which would then allow the attacker to manipulate network configuration for the SD-WAN fabric.

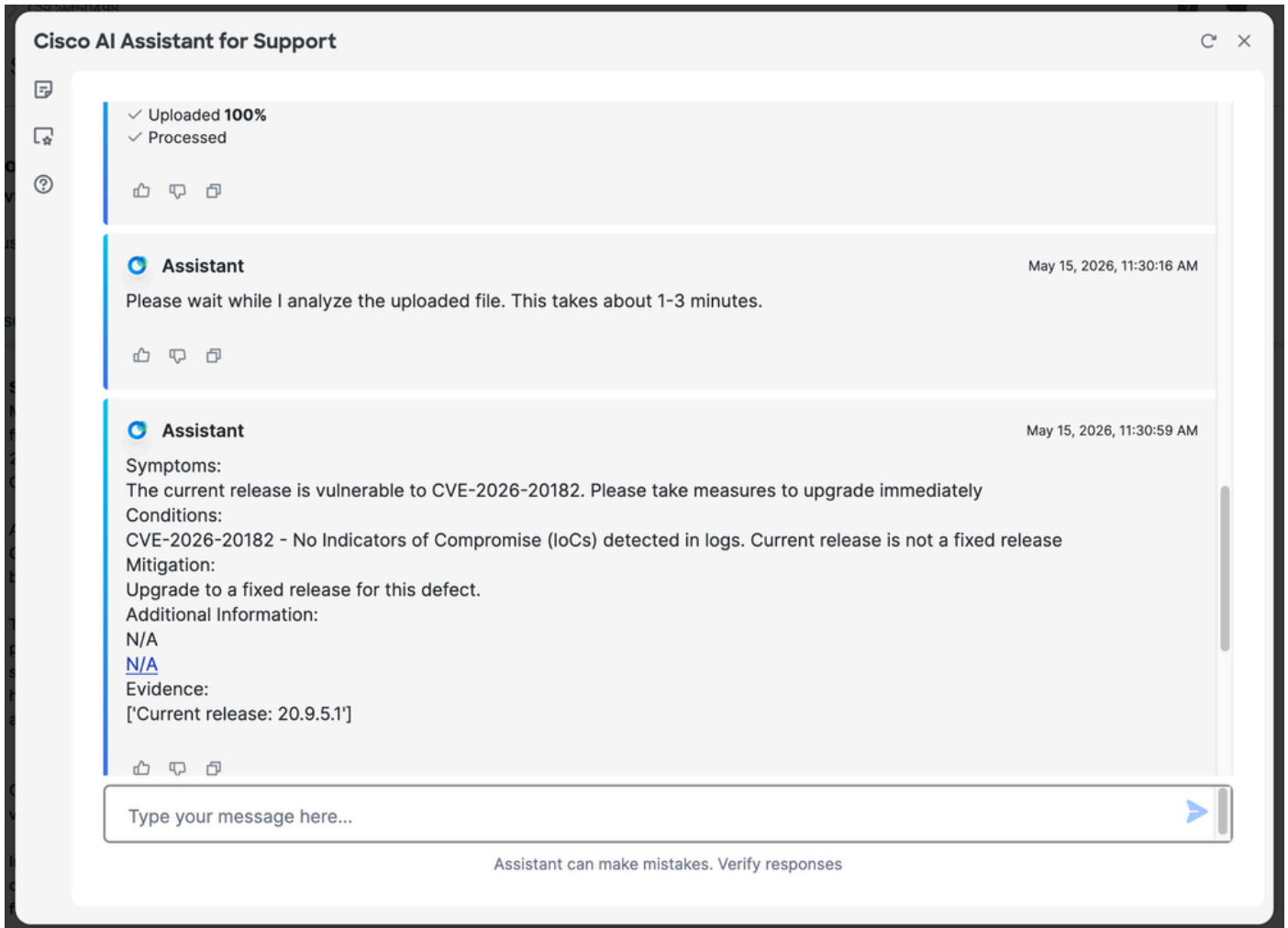
Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.

Important: To preserve possible indicators of compromise, customers should issue the request admin-tech command from each of the control components in the SD-WAN deployment before upgrading. After the admin-tech file has been collected, software should be upgraded at the earliest opportunity.

## Ergebnisse - Keine Indikatoren

Wenn keine Indikatoren gefunden werden, wird eine Meldung wie "CVE-2026-20182 - No Indicators of Compromise (IoCs)" in Protokollen erkannt. Die aktuelle Version ist keine feste Version." wird angezeigt. Die Nachricht verweist auf die spezielle Bug-ID, die analysiert wird.

Anmerkung: Wenn Sie noch kein Upgrade durchgeführt haben, fahren Sie bitte fort und aktualisieren Sie sofort auf eine Version, die das Fix enthält.



## Ergebnisse - gefundene Indikatoren

Wenn das Tool Indikatoren findet, wird die Meldung "Potenzielle Indicators of Compromise (IoCs) erkannt" angezeigt.

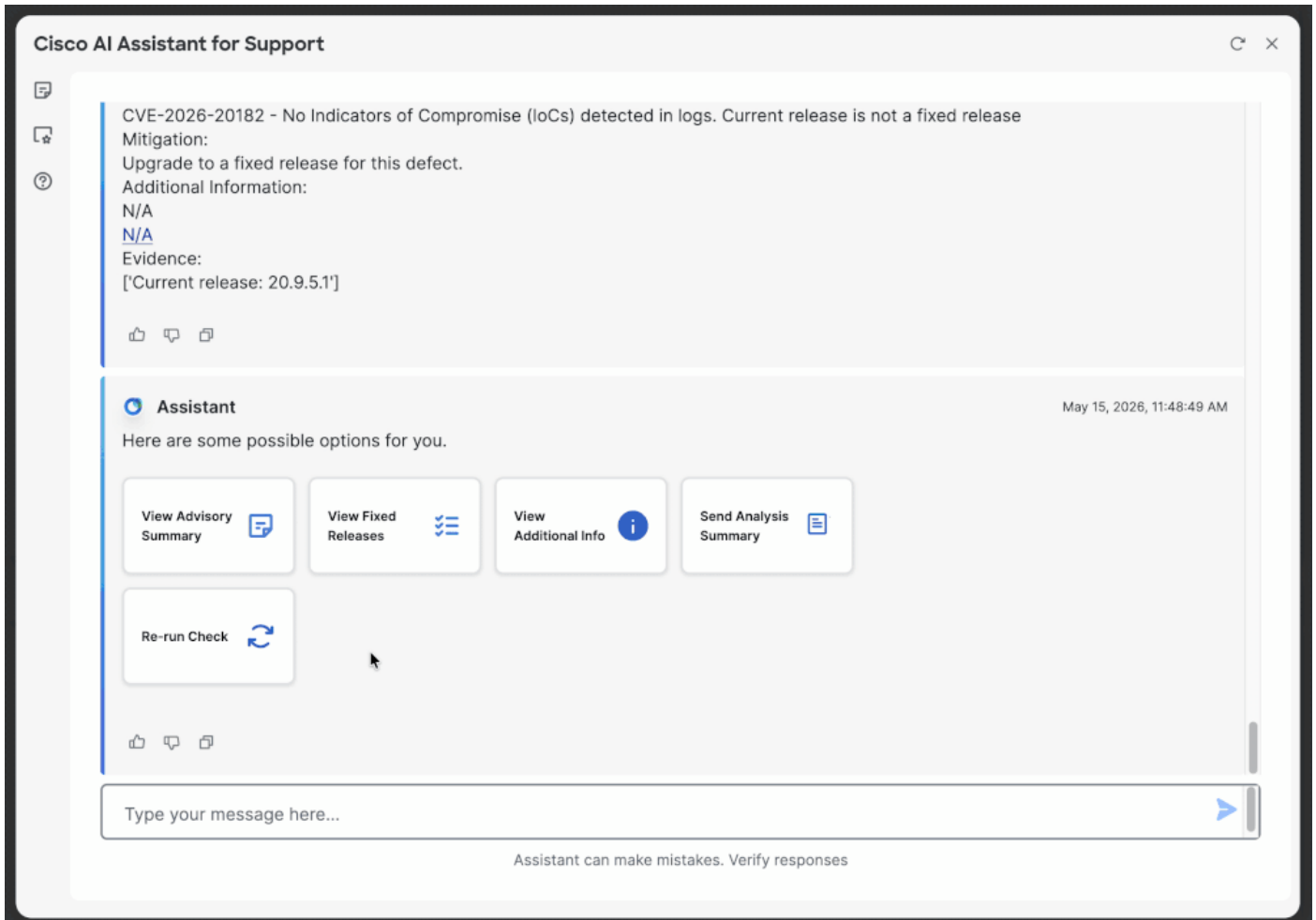
[Öffnen](#) Sie [ein Cisco TAC-Ticket](#), und laden Sie die Admin-Techniker hoch, um sie manuell überprüfen zu lassen.

Anmerkung: Wenn Sie noch kein Upgrade durchgeführt haben, fahren Sie bitte fort und aktualisieren Sie sofort auf eine Version, die das Fix enthält.



## Analyse einer zusätzlichen Admin-Tech

Um einen anderen Admin-Techniker zu analysieren, klicken Sie auf "Re-run" und geben Sie die entsprechende Cisco Bug-ID ein (z. B. [CSCwt50498](#)), um den Upload-Abschnitt erneut anzuzeigen. Weitere Optionen sind Scrollen nach oben und Klicken auf "Check <Bug ID>" oder Eingeben der Bug ID in den Chat.



## Zusätzliche Optionen

Nach der Analyse eines Admin-Tech, sind diese zusätzlichen Optionen im Tool verfügbar:

- Beratende Zusammenfassung anzeigen
  - Fixed Releases anzeigen
  - Weitere Informationen anzeigen
  - Analysezusammenfassung senden
-

## 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.