

Verifica della porta SD-WAN PSIRT con lo strumento Check Bug Applicability

Sommario

[Introduzione](#)

[Requisiti](#)

[Linee guida per la generazione di tecnologie di amministrazione](#)

[Limitazioni](#)

[Utilizzo](#)

[Verifica di una configurazione Admin-Tech](#)

[Risultati - Nessun indicatore](#)

[Risultati - Indicatori trovati](#)

[Analisi di un'ulteriore tecnologia di amministrazione](#)

[Ulteriori opzioni disponibili](#)

Introduzione

Questo documento descrive come usare lo strumento Bug Applicability per analizzare i file admin-tech alla ricerca di possibili indicatori di compromessi (IoC) relativi a SD-WAN Product Security Incident Response Team (PSIRT) CVE-2026-20182 [CSCwt50498](#)

Requisiti

Per [CSCwt50498](#), è necessario generare un admin-tech dei componenti di controllo SD-WAN. Gli admin-tech del controller (vSmart) devono essere generati uno alla volta.

Gli admin-tech degli altri componenti di controllo SD-WAN possono essere generati in qualsiasi ordine.

Linee guida per la generazione di tecnologie di amministrazione

Per assistenza nella creazione di questi file, fare riferimento a questo documento in cui vengono illustrati i passaggi per generare un file admin-tech: [Come raccogliere un admin-tech in un ambiente SD-WAN](#).

Limitazioni

- Le dimensioni del file sono attualmente limitate a 500 MB.
- Verifica simultanea dei file non supportata. Lo strumento può elaborare più file, ma solo uno alla volta.

Utilizzo

Verifica di una configurazione Admin-Tech

1. Andare alla pagina Cisco Bug Search Tool per l'ID bug Cisco che si desidera analizzare.
2. Sotto il titolo, fare clic sul testo o sull'icona "Check Bug Applicability" (Verifica dell'applicabilità del bug). Viene visualizzata una finestra popup.
3. Eliminare o selezionare il file admin-tech che si desidera analizzare.

 > CSCwt50498



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.

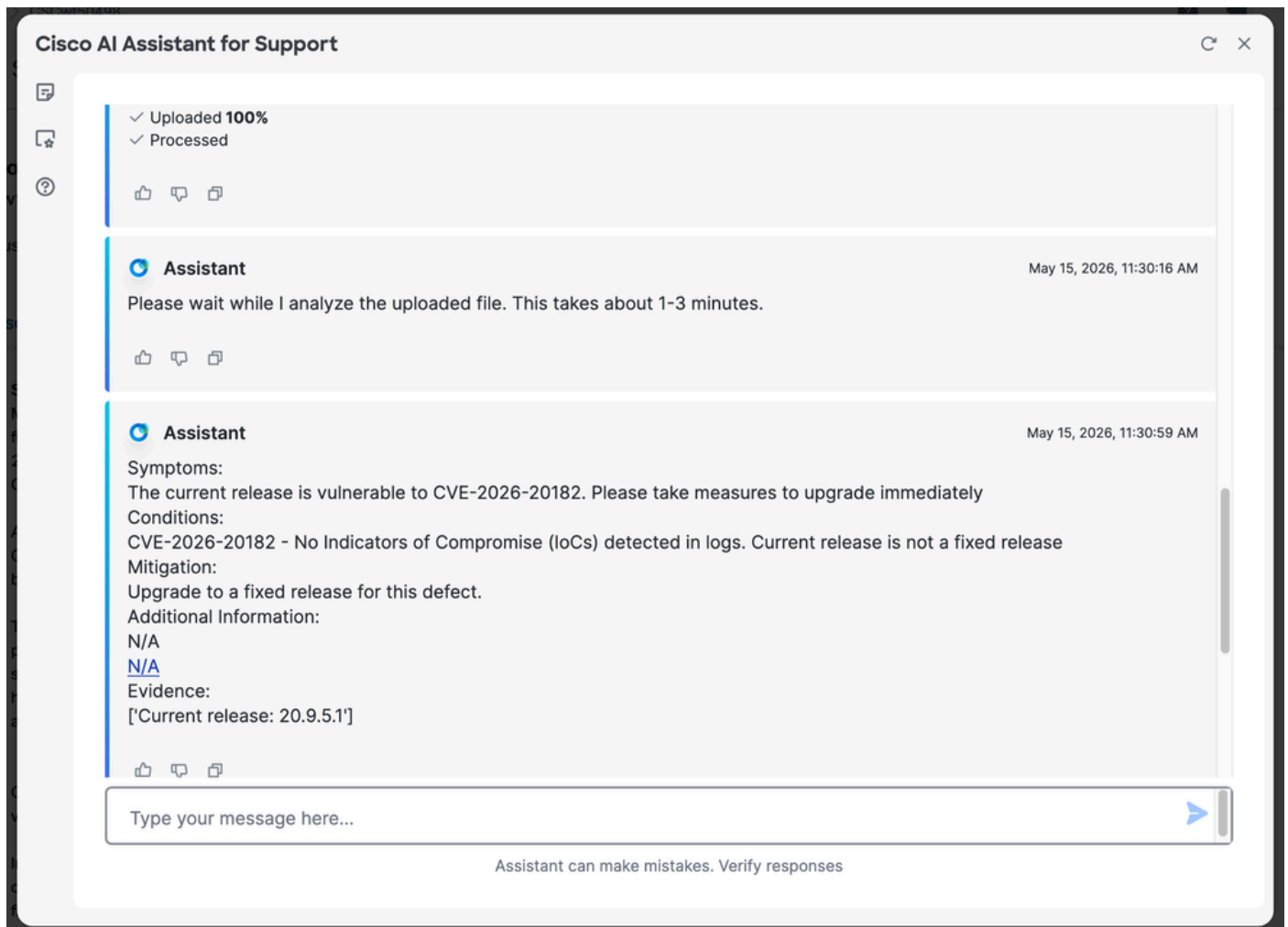
Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.

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.

Risultati - Nessun indicatore

Se non vengono rilevati indicatori, viene visualizzato un messaggio simile a "CVE-2026-20182 - No Indicators of Compromise (IoCs) detected in logs. Current release is not a fixed release" (La versione corrente non è fissa). Il messaggio farà riferimento all'ID bug specifico analizzato.

Nota: Se non è stato ancora eseguito l'aggiornamento, procedere immediatamente e passare a una release contenente la correzione.



Risultati - Indicatori trovati

Se lo strumento trova degli indicatori, appare il messaggio "Potential Indicators of Compromise (IoCs) Detected" (Indicatori potenziali di compromesso rilevati).

Apri [una richiesta Cisco TAC](#) e carica gli admin-tech per un'ulteriore revisione manuale.

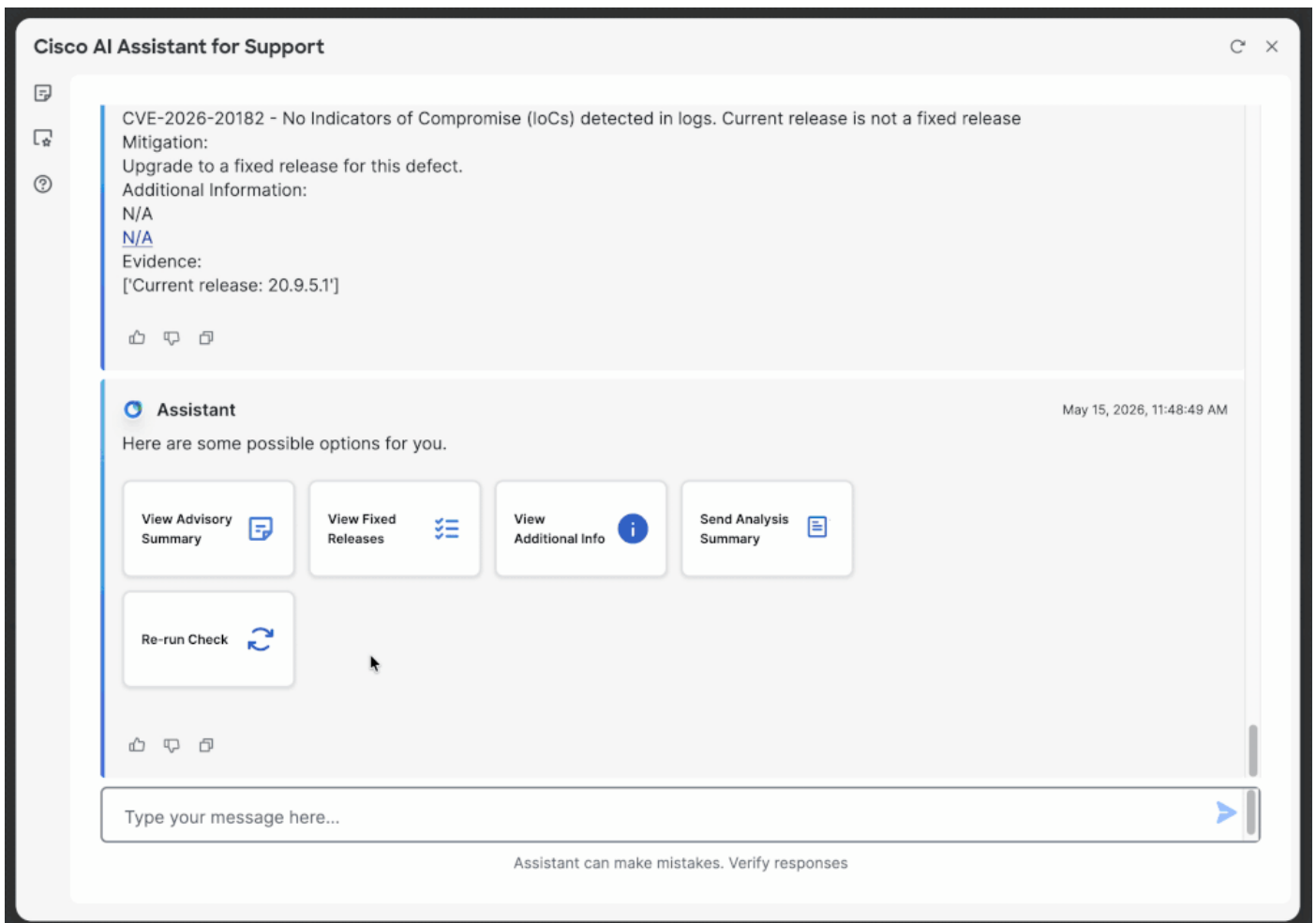
Nota: Se non è stato ancora eseguito l'aggiornamento, procedere immediatamente e passare a

una release contenente la correzione.



Analisi di un'ulteriore tecnologia di amministrazione

Per analizzare un'altra tecnologia avanzata, fare clic su "Re-run" (Esegui di nuovo) e immettere l'ID bug Cisco applicabile (ad esempio, [CSCwt50498](#)) per visualizzare di nuovo la sezione di caricamento. Altre opzioni includono lo scorrimento verso l'alto e la selezione di "Controlla <ID bug>" o l'immissione dell'ID del bug nella chat.



Ulteriori opzioni disponibili

Dopo aver analizzato un admin-tech, queste opzioni aggiuntive sono disponibili nello strumento:

- Visualizza riepilogo advisory
 - Visualizza rilasci fissi
 - Visualizza informazioni aggiuntive
 - Invia riepilogo analisi
-

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).