

Verify SD-WAN PSIRT with the Check Bug Applicability Tool

Contents

[Introduction](#)

[Requirements](#)

[Admin-Tech Generation Guidelines](#)

[Limitations](#)

[Utilization](#)

[Verify an Admin-Tech](#)

[Results - No Indicators](#)

[Results - Indicators Found](#)

[Analyze an Additional Admin-Tech](#)

[Additional Options Available](#)

Introduction

This document describes how to use the **Bug Applicability** tool to scan admin-tech files for possible Indicators of Compromise (IoCs) related to SD-WAN Product Security Incident Response Team (PSIRT) CVE-2026-20182 [CSCwt50498](#)

Requirements

For [CSCwt50498](#), you must generate an admin-tech of your SD-WAN control components. **The Controller (vSmart) admin-techs must be generated one at a time.**

The admin-techs of other SD-WAN control components can be generated in any order.

Admin-Tech Generation Guidelines

If you need assistance creating these files, please refer to the this document that provides the steps to generate an admin-tech: [How to Collect an Admin-Tech in an SD-WAN Environment](#).

Limitations

- The file size is currently limited to 500 MB.
- Simultaneous file verification is not supported. The tool can process multiple files, but only one at a time.

Utilization

Verify an Admin-Tech

1. Go to the Cisco Bug Search Tool page for the Cisco Bug ID you want to analyze.
2. Under the title, click on the text or icon "**Check Bug Applicability**". A pop-up window appears.
3. Drop or select the admin-tech file you want to analyze.

 > 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.

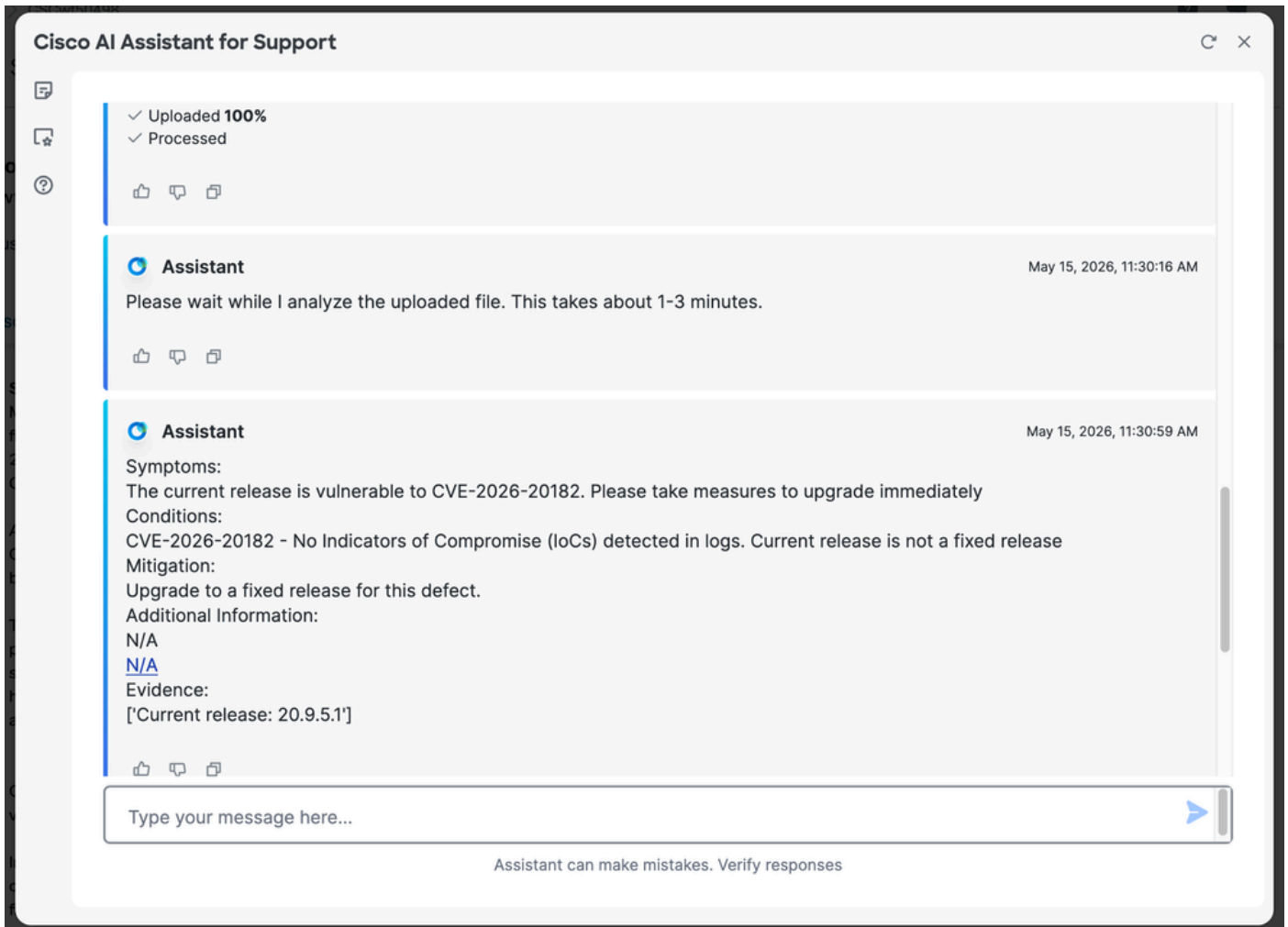
Important: To preserve possible indicators of compromise, customers should issue the request admin-tech command from each of the control components in the SD-WAN deployment before upgrading. After the admin-tech file has been collected, software should be upgraded at the earliest opportunity.

Results - No Indicators

If no indicators are found, a message similar to "**CVE-2026-20182 - No Indicators of Compromise (IoCs)**"

detected in logs. Current release is not a fixed release" appears. The message will reference the specific Bug ID being analyzed.

Note: If you have not upgraded yet, please proceed and upgrade immediately to a release containing the fix.



Results - Indicators Found

If the tool finds indicators, the message "**Potential Indicators of Compromise (IoCs) Detected**" appears.

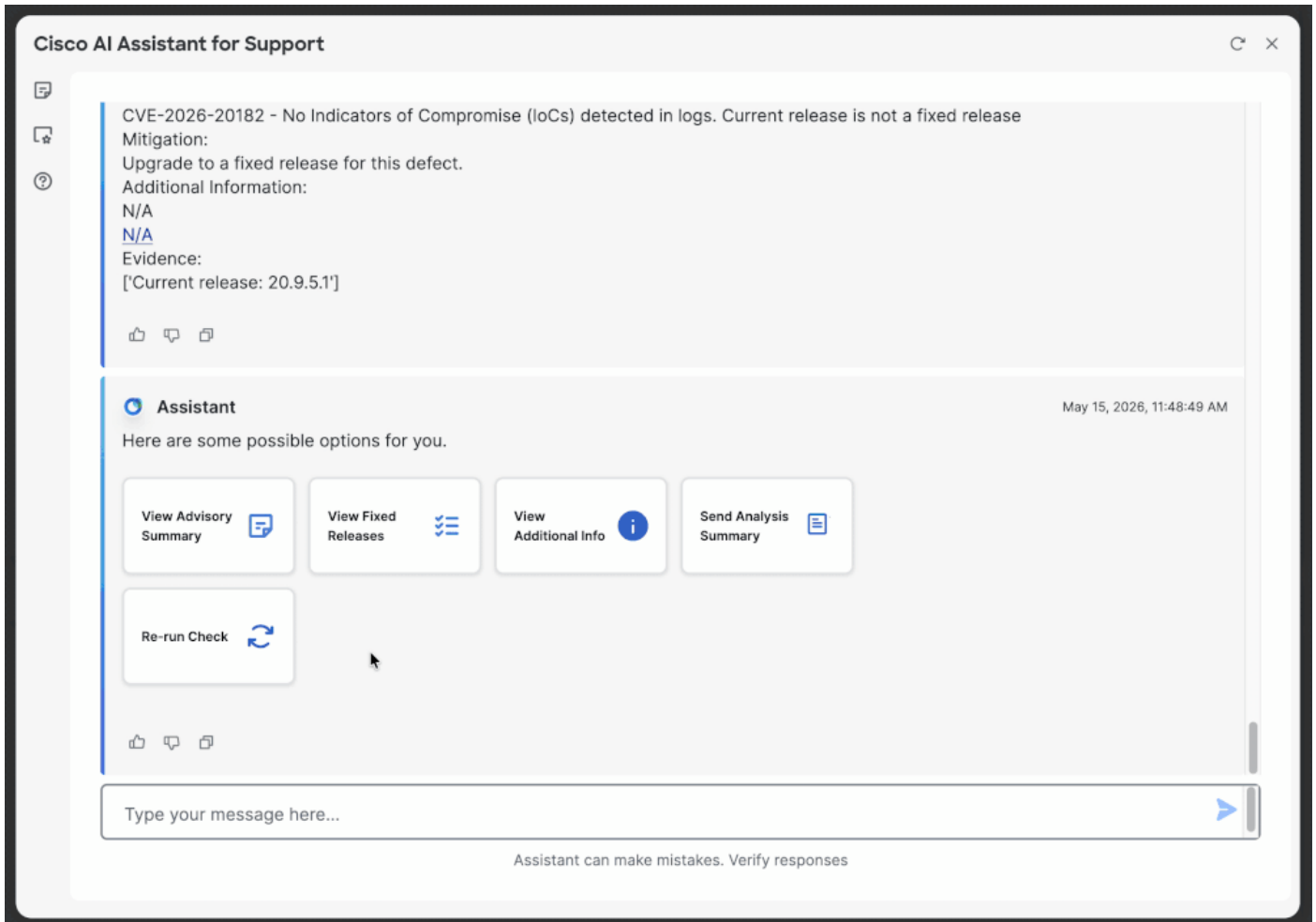
Please [open a Cisco TAC case](#) and upload the admin-techs for further manual review.

Note: If you have not upgraded yet, please proceed and upgrade immediately to a release containing the fix.



Analyze an Additional Admin-Tech

To analyze another admin-tech, click "Re-run" and enter the applicable Cisco Bug ID (e.g., [CSCwt50498](#)) to see the upload section again. Other options include scrolling up and clicking "**Check <Bug ID>**" or typing the bug ID into the chat.



Additional Options Available

After analyzing an admin-tech, these additional options are available in the tool:

- View Advisory Summary
 - View Fixed Releases
 - View Additional Info
 - Send Analysis Summary
-