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-2026-20182CSCwt50498**

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.



Warning: Before upgrading an SD-WAN deployment to a fixed release, retain relevant logs. After upgrading, verify that the system has not been compromised, by checking the logs for the indicators of compromise as documented in these advisories. If the logs show indicators of compromise and you confirm that your system has been compromised, applying the software update alone will not resolve the vulnerability. In such cases, follow the specific remediation steps that are provided by the Cisco Technical Assistance Center (TAC) to help secure the system.

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.

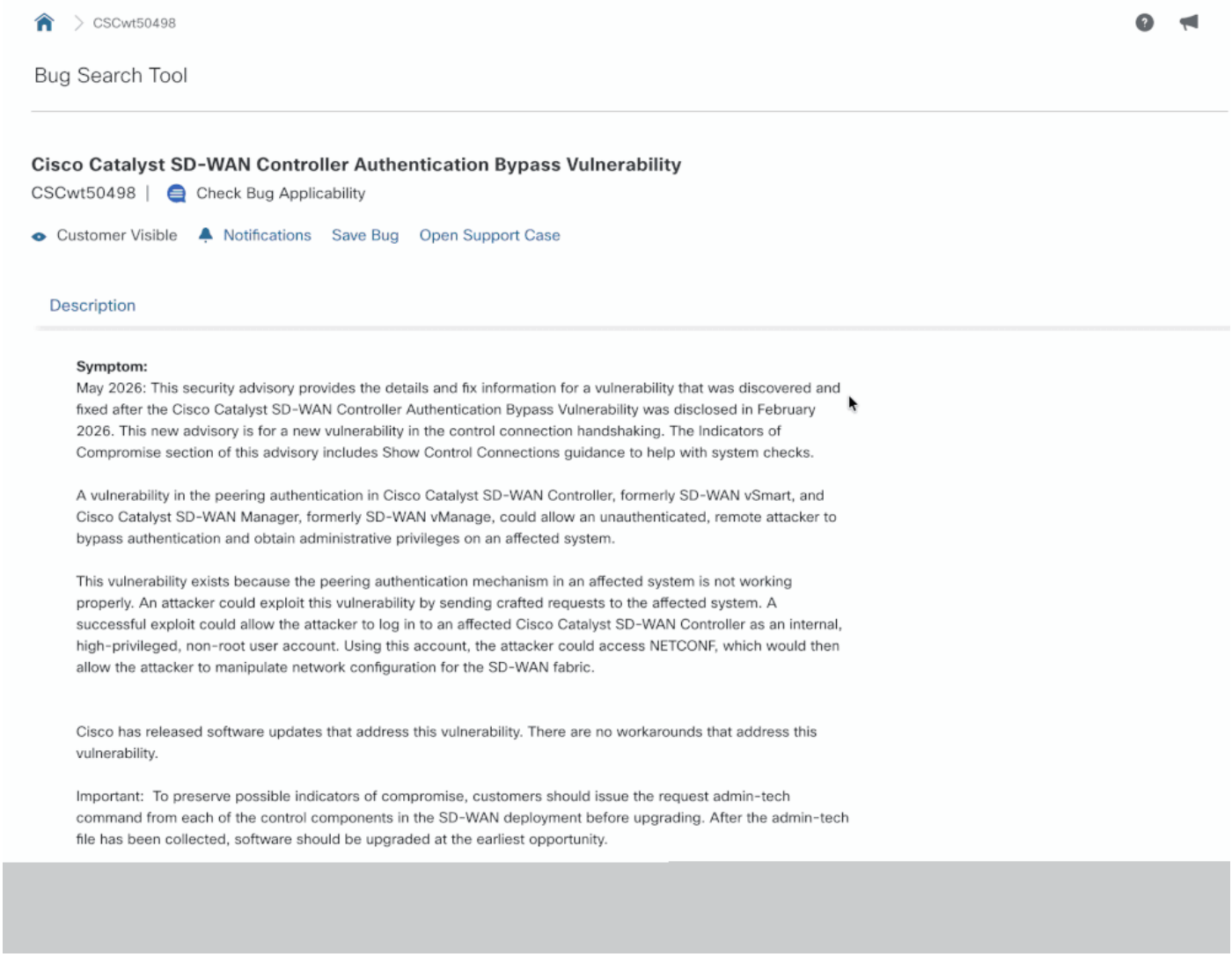
Limitations

- 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

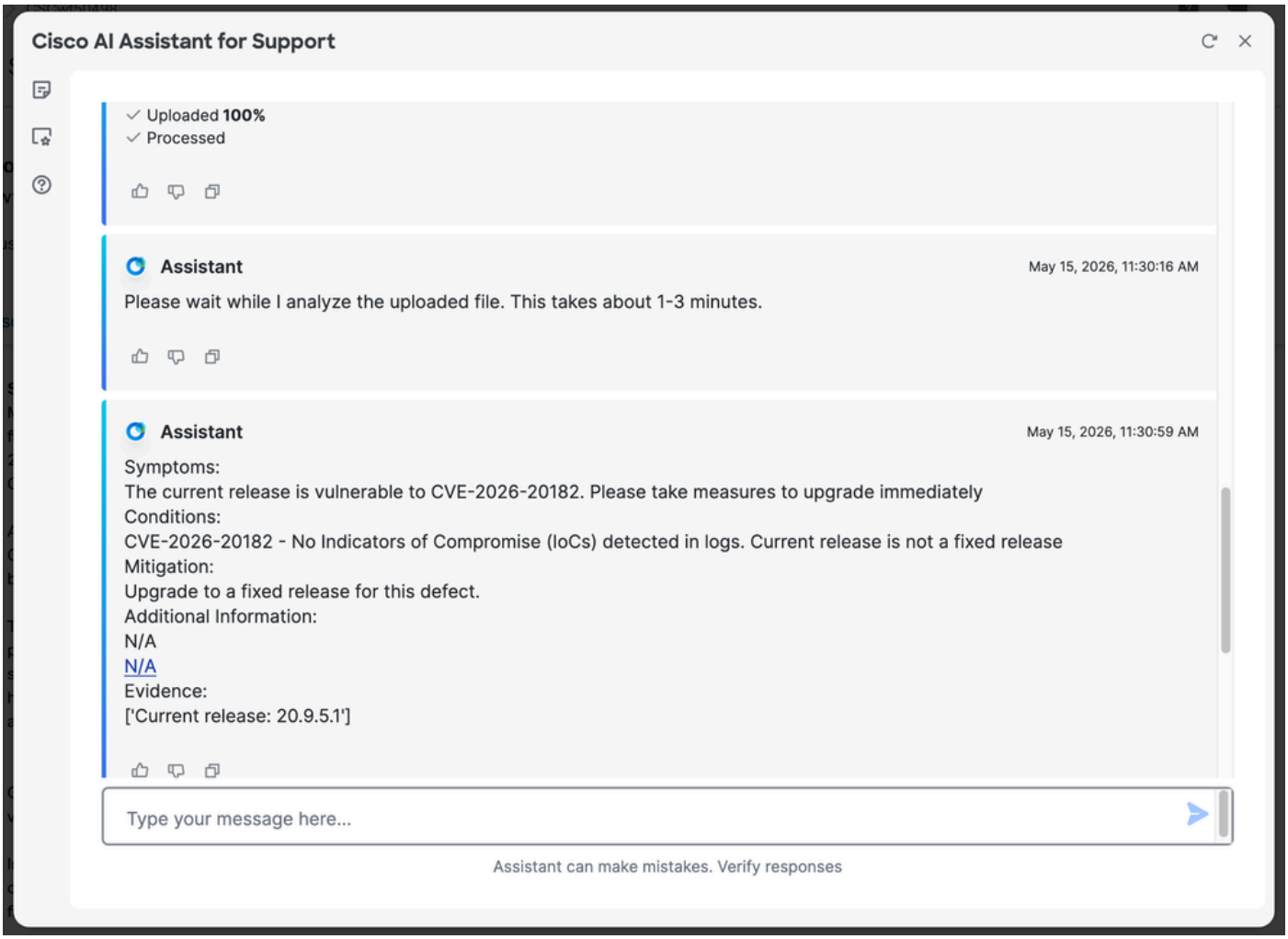
1. Go to the Cisco Bug Search Tool page for the Cisco Bug ID you want to analyze.
2. Under the title, click on the text or icon "**Check Bug Applicability**". A pop-up window appears.
3. Drop or select the admin-tech file you want to analyze.



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.

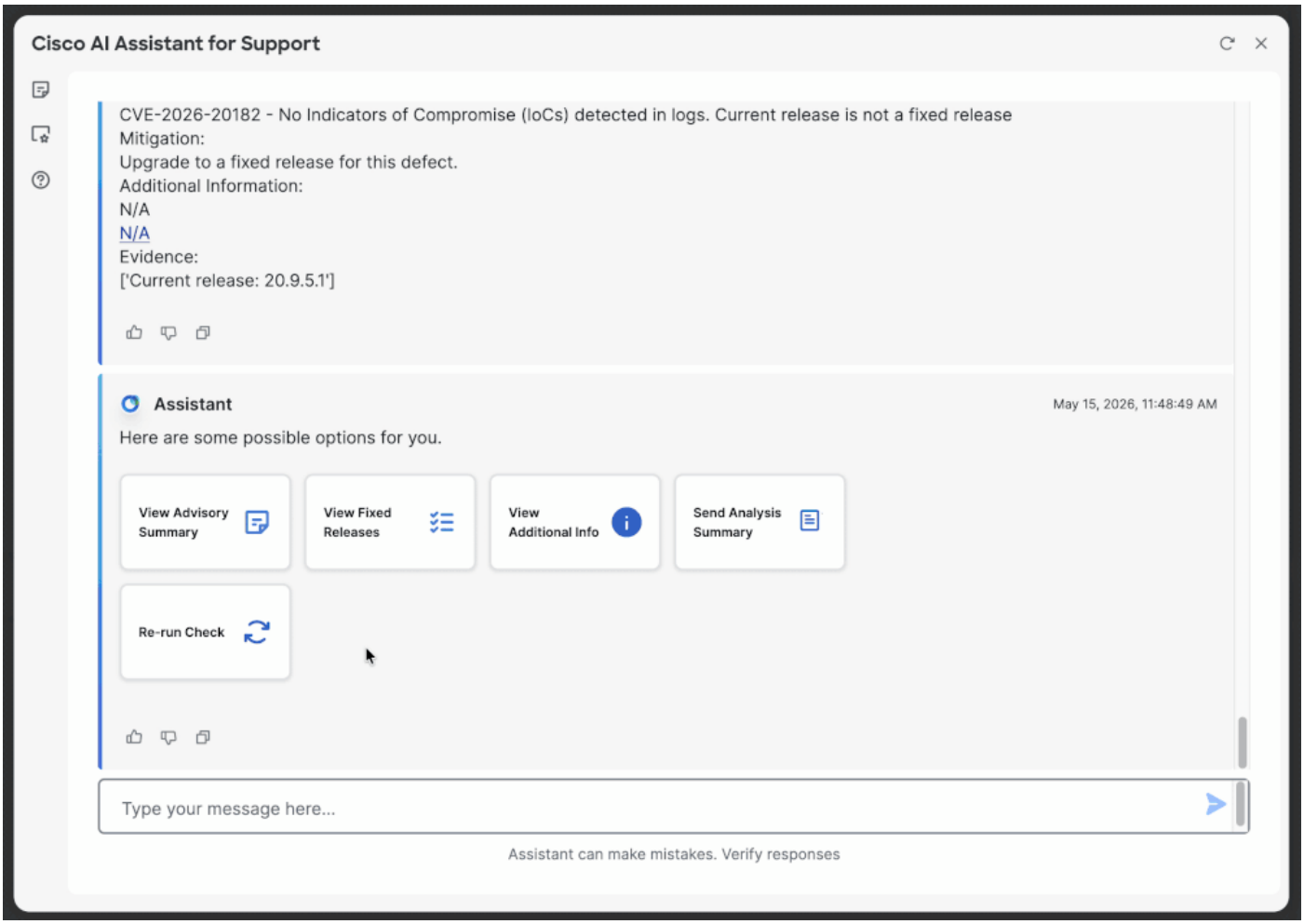
Please open a Cisco TAC case and upload the admin-techs for further manual review.

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
