

使用檢查錯誤適用性工具驗證SD-WAN PSIRT

目錄

[簡介](#)

[需求](#)

[管理技術生成指南](#)

[限制](#)

[利用率](#)

[驗證管理技術](#)

[結果 — 無指標](#)

[結果 — 找到的指示符](#)

[分析其他管理技術](#)

[可用的其他選項](#)

簡介

本檔案介紹如何使用Bug Applicability工具掃描管理技術檔案，以瞭解與SD-WAN產品安全事件響應團隊(PSIRT)CVE-2026-20182CSCwt50498相關的[可能危害表現\(loC\)](#)

需求

對於[CSCwt50498](#)，必須生成SD-WAN控制元件的管理技術。每次必須生成一個控制器(vSmart)管理技術。

其他SD-WAN控制元件的管理技術可以按任意順序生成。

管理技術生成指南

如果您需要建立這些檔案方面的幫助，請參閱本文提供的生成管理技術檔案的步驟：[如何在SD-WAN環境中收集管理技術](#)。

限制

- 檔案大小目前限制為500 MB。
- 不支援同時檔案驗證。該工具可以處理多個檔案，但一次只能處理一個檔案。

利用率

驗證管理技術

1. 前往思科錯誤搜尋工具頁面，尋找您要分析的思科錯誤ID。
2. 在標題下，按一下文字或圖示「Check Bug Applicability(檢查錯誤適用性)」。系統將顯示一個彈出視窗。
3. 刪除或選擇要分析的管理技術檔案。

 > 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.

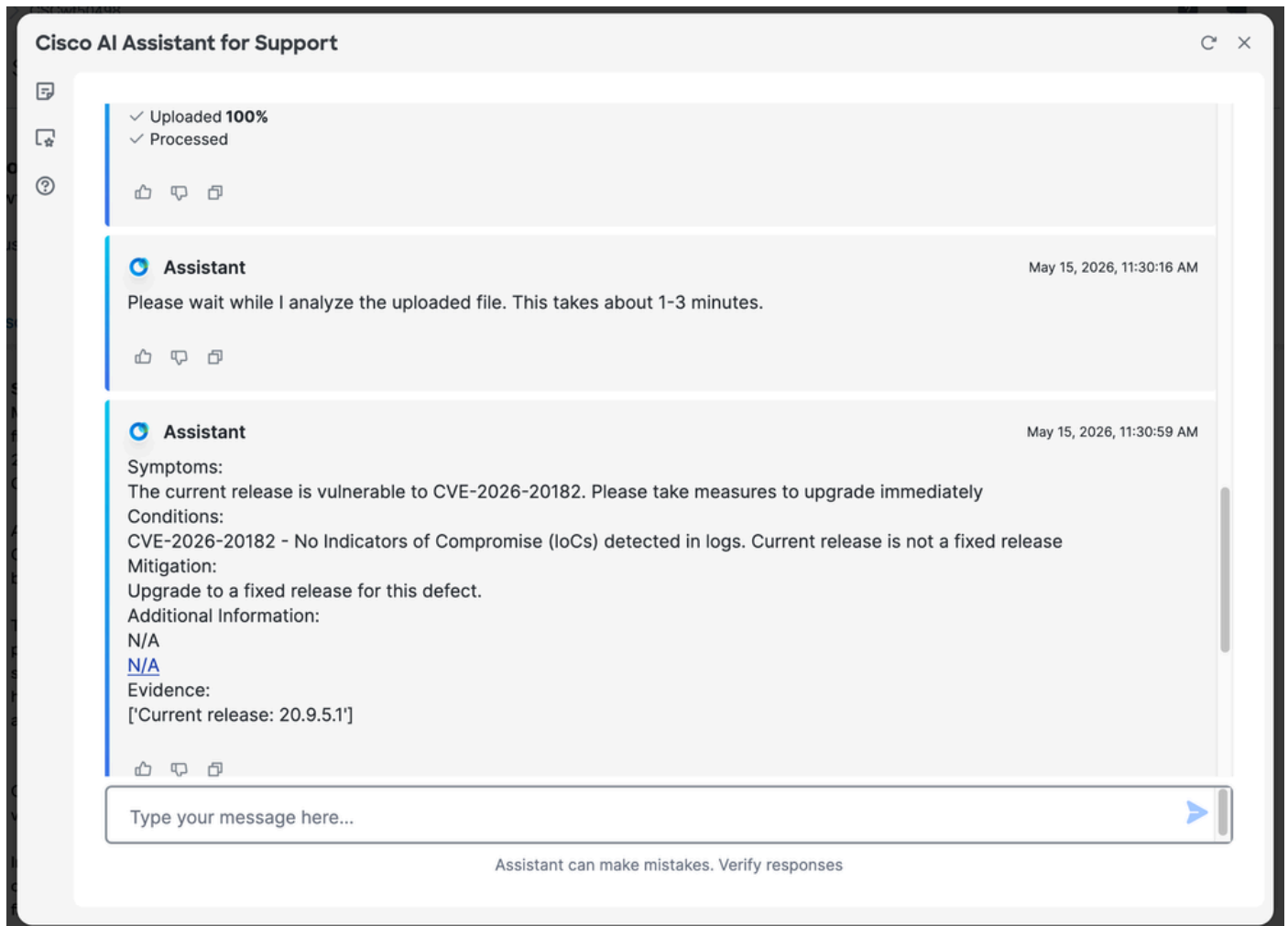
Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.

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.

結果 — 無指標

如果未找到指示符，則在日誌中檢測到類似於「CVE-2026-20182 — 無危害指示符(IoC)」的消息。系統會顯示目前版本不是固定版本「」。該訊息將參考正在分析的特定錯誤ID。

附註：如果您尚未升級，請立即繼續並升級到包含修復程式的版本。



結果 — 找到的指示符

如果工具找到指示符，將顯示消息「Possible Indicators of Compromise(IoC)Detected」。

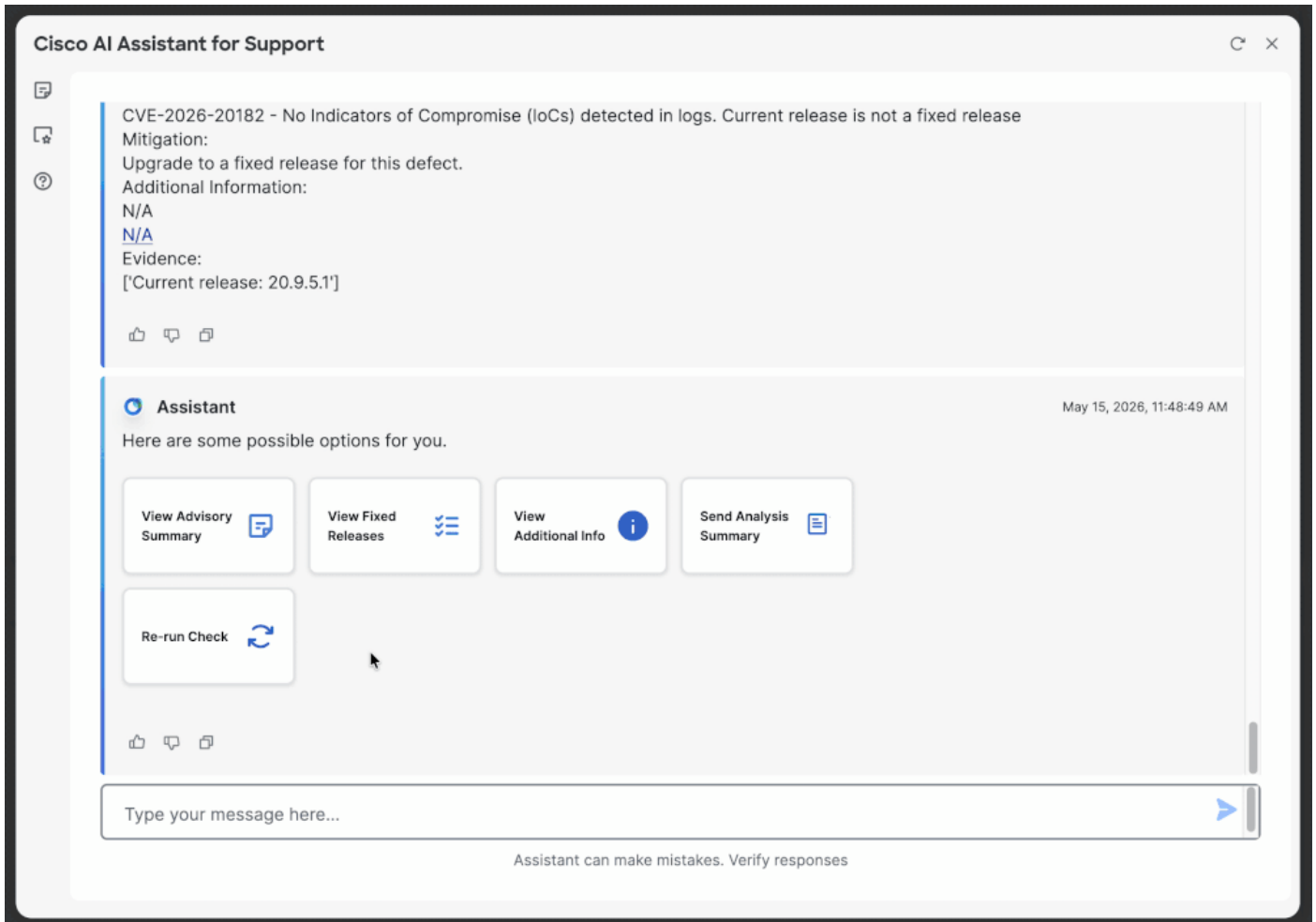
請開[啟思科TAC案例](#)，並上傳管理技術人員，以供進一步手動稽核。

附註：如果您尚未升級，請立即繼續並升級到包含修復程式的版本。



分析其他管理技術

若要分析另一個管理技術，請按一下「Re-run」，然後輸入適用的思科錯誤ID(例如，[CSCwt50498](#))，以再次檢視上傳部分。其他選項包括向上滾動並單擊「檢查<Bug ID>」或在聊天中輸入錯誤ID。



可用的其他選項

分析管理技術後，該工具中提供了以下附加選項：

- 檢視建議摘要
- 檢視修正版本
- 檢視其他資訊
- 傳送分析摘要

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。