

# Check Bug Applicability ToolによるSD-WAN PSIRTの確認

## 内容

---

[はじめに](#)

[要件](#)

[Admin-Tech Generationガイドライン](#)

[制限事項](#)

[使用率の向上](#)

[Admin-Techの確認](#)

[結果 - インジケータなし](#)

[結果 - 検出されたインジケータ](#)

[追加のAdmin-Techの分析](#)

[追加オプションを利用可能](#)

---

## はじめに

このドキュメントでは、Bug Applicabilityツールを使用して、SD-WAN Product Security Incident Response Team(PSIRT)CVE-2026-20182に関連する潜在的な侵害の指標(IOC)についてadmin-techファイルをスキャンする方法について説明しCSCwt50498す。

## 要件

[CSCwt50498](#)の場合、SD-WAN制御コンポーネントのadmin-techを生成する必要があります。コントローラ(vSmart)の管理テクノロジーは、1つずつ生成する必要があります。

他のSD-WAN制御コンポーネントのadmin-techsは、任意の順序で生成できます。

## Admin-Tech Generationガイドライン

これらのファイルの作成でサポートが必要な場合は、このドキュメントでadmin-techの生成手順を参照してください([SD-WAN環境でAdmin-Techを収集する方法](#))。

# 制限事項

- ファイルサイズは現在500 MBに制限されています。
- 同時ファイル検証はサポートされていません。このツールでは複数のファイルを処理できませんが、一度に処理できるのは1つだけです。

# 使用率の向上

## Admin-Techの確認

1. Cisco Bug Search Toolページにアクセスし、分析するCisco Bug IDを探します。
2. タイトルの下にあるテキストまたはアイコン「Check Bug Applicability」をクリックします。ポップアップウィンドウが表示されます。
3. 分析するadmin-techファイルをドロップするか選択します。

🏠 > 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.

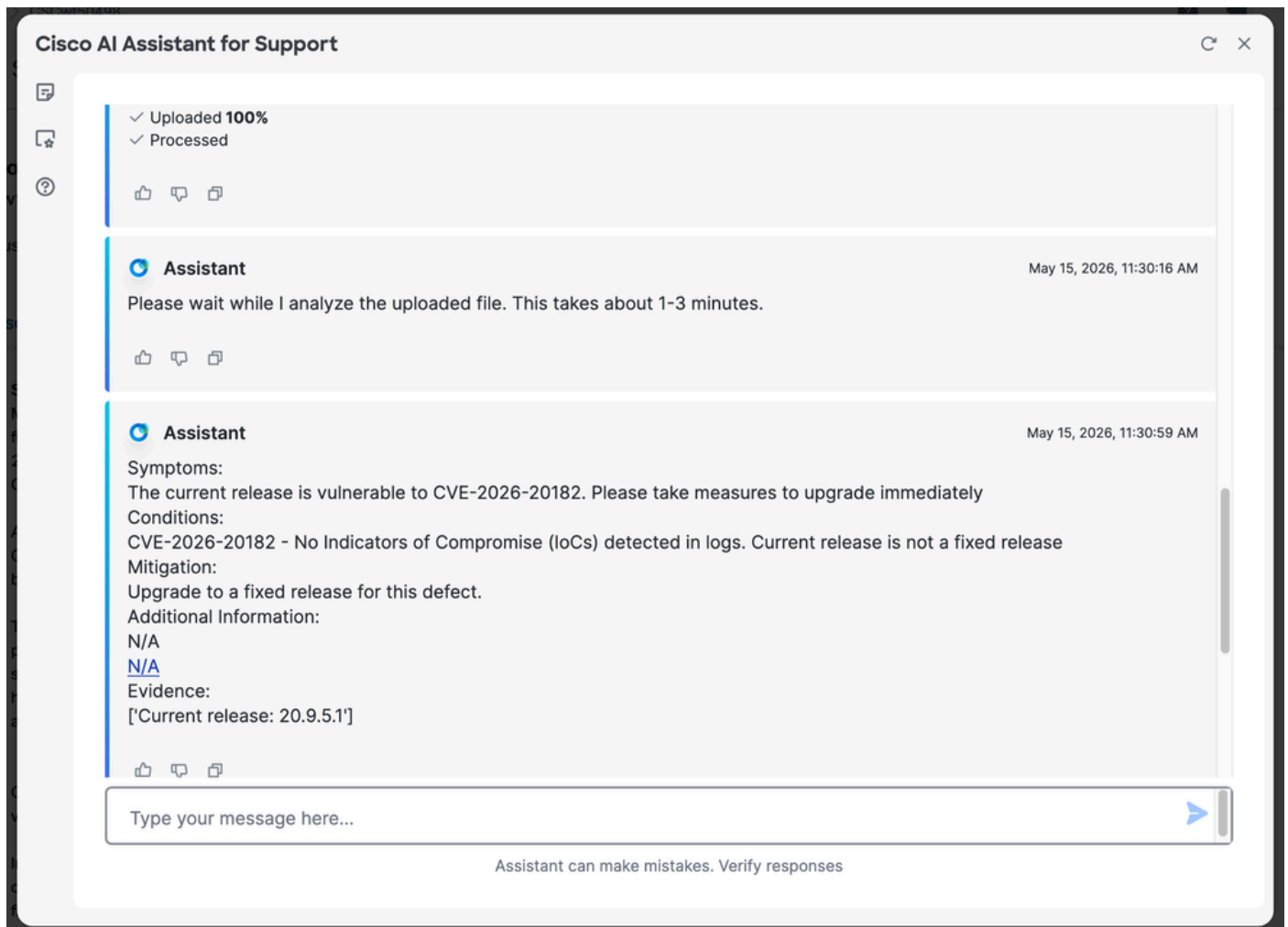
Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.

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 – インジケータなし

インジケータが見つからない場合は、「CVE-2026-20182 - No Indicators of Compromise (IoCs) detected in logs」のようなメッセージが表示されます。Current release is not a fixed release」が表示されます。このメッセージは、分析中の特定のバグIDを参照します。

注：まだアップグレードしていない場合は、先に進み、修正を含むリリースにただちにアップグレードしてください。

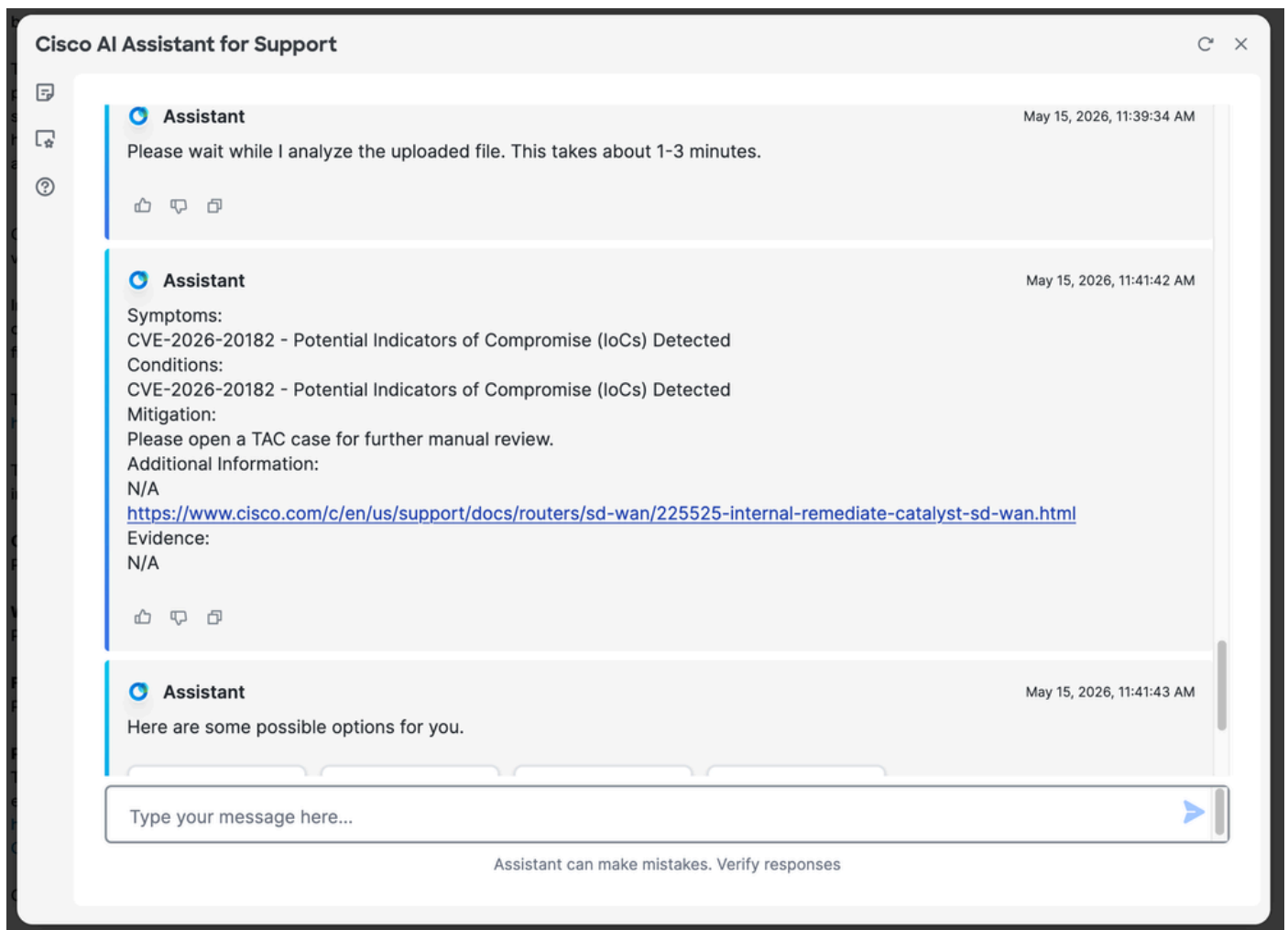


## 結果 – 検出されたインジケータ

インジケータが検出されると、「Potential Indicators of Compromise (IoCs) Detected」というメッセージが表示されます。

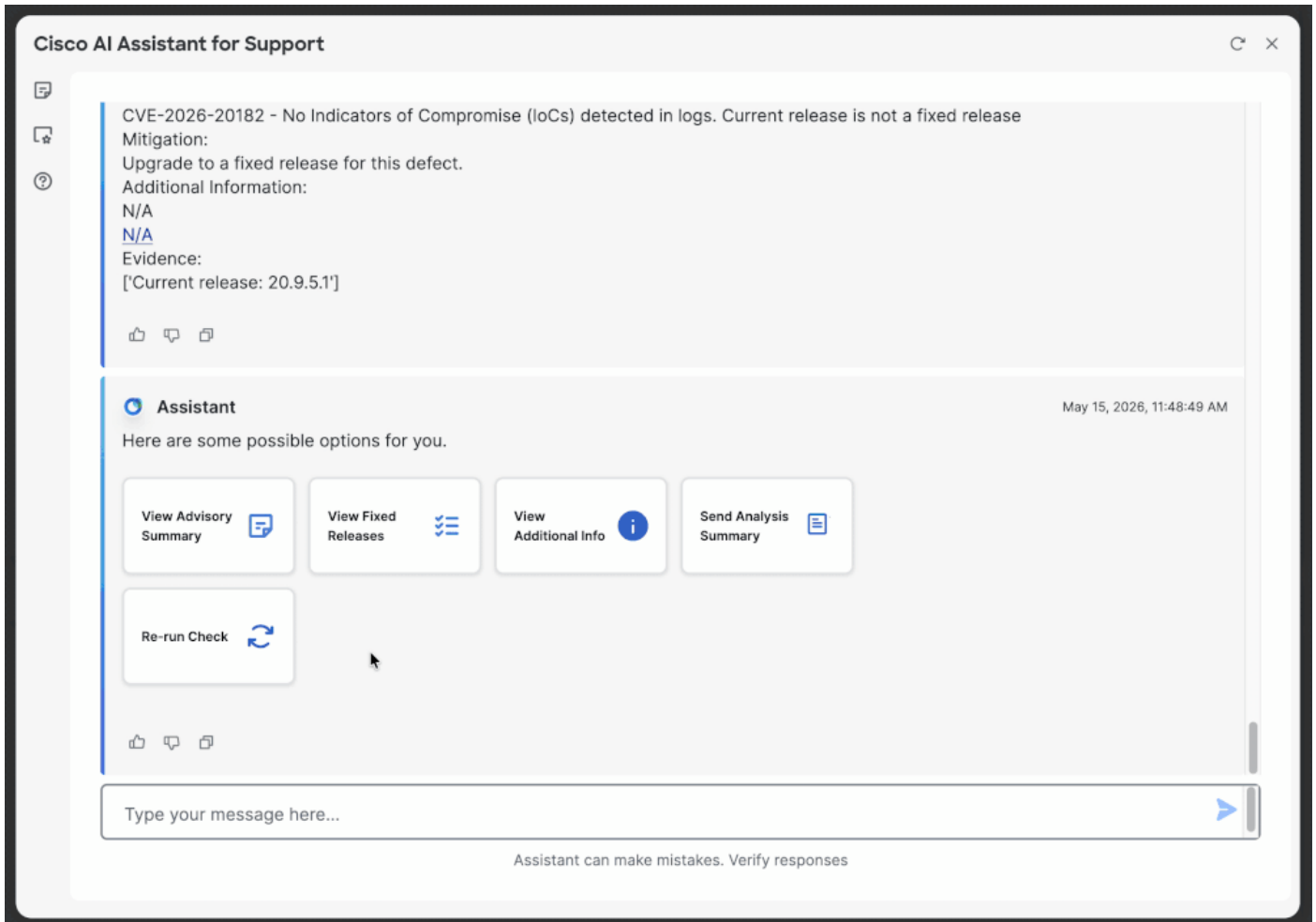
[Cisco TACケースを開き](#)、さらに手動でレビューするために管理者テクニックをアップロードしてください。

注：まだアップグレードしていない場合は、先に進み、修正を含むリリースにただちにアップグレードしてください。



## 追加のAdmin-Techの分析

別のadmin-techを分析するには、「再実行」をクリックし、該当するCisco Bug ID(例：[CSCwt50498](#))を入力して、アップロードセクションを再度表示します。その他のオプションには、スクロールアップして「Check <Bug ID>」をクリックする方法や、チャットでバグIDを入力する方法があります。



## 追加オプションを利用可能

admin-techを分析した後、ツールで次の追加オプションを使用できます。

- アドバイザリサマリーの表示
- 修正済みリリースの表示
- 追加情報の表示
- 分析サマリーの送信

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。