

# Vérification du PSIRT SD-WAN avec l'outil Check Bug Applicability Tool

## Table des matières

---

[Introduction](#)

[Exigences](#)

[Instructions de génération Admin-Tech](#)

[Limites](#)

[Utilisation](#)

[Vérification d'un Admin-Tech](#)

[Résultats - Aucun indicateur](#)

[Résultats - Indicateurs trouvés](#)

[Analyser un Admin-Tech supplémentaire](#)

[Options supplémentaires disponibles](#)

---

## Introduction

Ce document décrit comment utiliser l'outil Bug Applicability pour analyser les fichiers admin-tech à la recherche d'indicateurs de compromission (IoC) possibles liés à l'équipe PSIRT (Product Security Incident Response Team) SD-WAN CVE-2026-20182 [CSCwt50498](#)

## Exigences

Pour [CSCwt50498](#), vous devez générer un admin-tech de vos composants de contrôle SD-WAN. Les admin-techs du contrôleur (vSmart) doivent être générées une par une.

Les admin-techs des autres composants de contrôle SD-WAN peuvent être générées dans n'importe quel ordre.

## Instructions de génération Admin-Tech

Si vous avez besoin d'aide pour créer ces fichiers, reportez-vous à ce document qui fournit les étapes pour générer un admin-tech : [Comment collecter un Admin-Tech dans un environnement SD-WAN](#).

## Limites

- La taille du fichier est actuellement limitée à 500 Mo.
- La vérification simultanée des fichiers n'est pas prise en charge. L'outil peut traiter plusieurs fichiers, mais un seul à la fois.

## Utilisation

### Vérification d'un Admin-Tech

1. Accédez à la page Outil de recherche de bogues Cisco pour l'ID de bogue Cisco que vous souhaitez analyser.
2. Sous le titre, cliquez sur le texte ou l'icône "Vérifier l'applicabilité du bogue". Une fenêtre contextuelle s'affiche.
3. Déposez ou sélectionnez le fichier admin-tech que vous souhaitez analyser.

## 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.

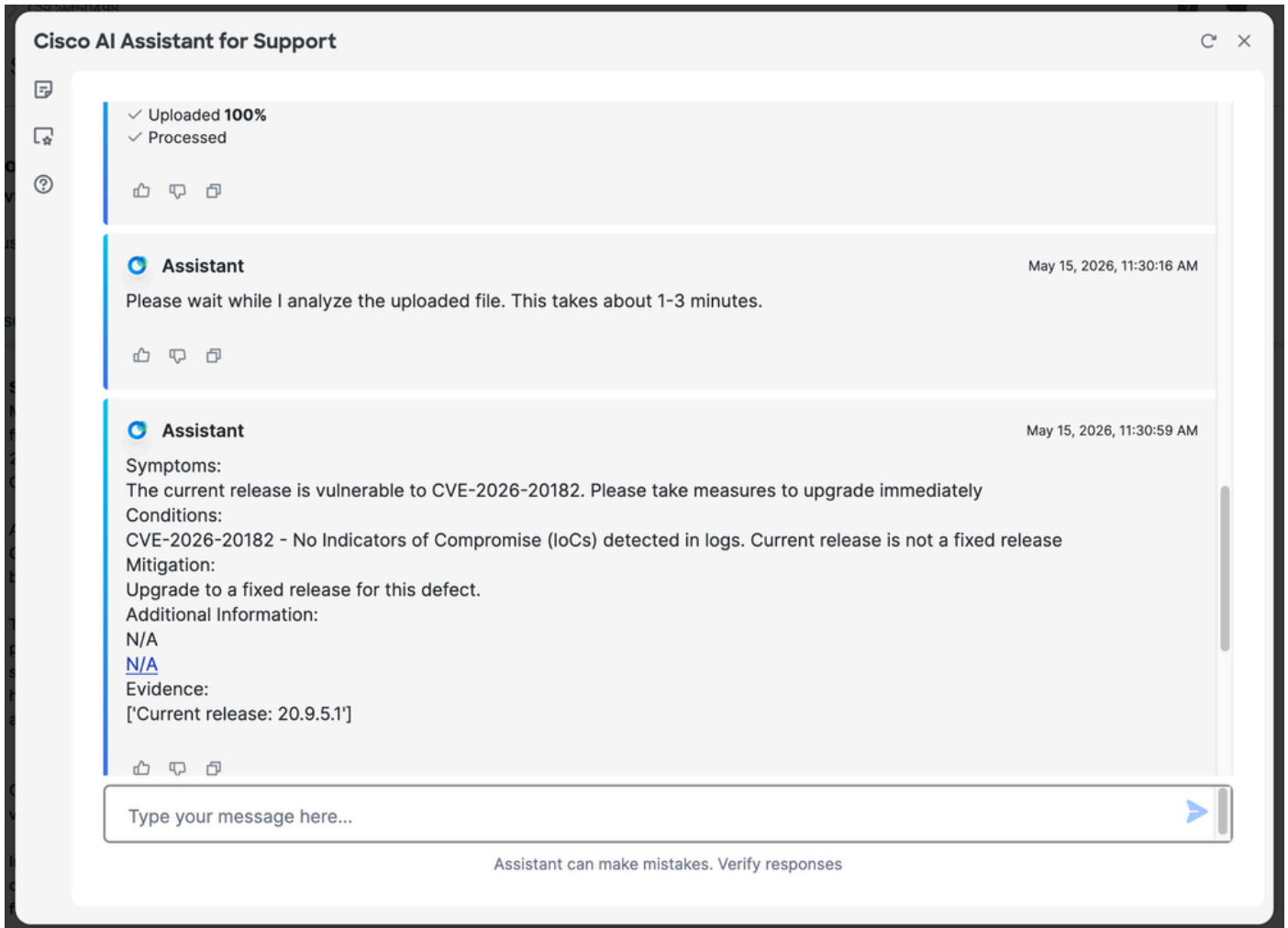
Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.

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.

## Résultats - Aucun indicateur

Si aucun indicateur n'est trouvé, un message semblable à « CVE-2026-20182 - No Indicators of Compromise (IoC) detected in logs » (CVE-2026-- Aucun indicateur de compromission (IoC) détecté dans les journaux). La version actuelle n'est pas une version fixe" s'affiche. Le message référencera l'ID de bogue spécifique en cours d'analyse.

Remarque : Si vous n'avez pas encore effectué la mise à niveau, veuillez procéder immédiatement à la mise à niveau vers une version contenant le correctif.



## Résultats - Indicateurs trouvés

Si l'outil détecte des indicateurs, le message « Indicateurs potentiels de compromission (IoC) détectés » s'affiche.

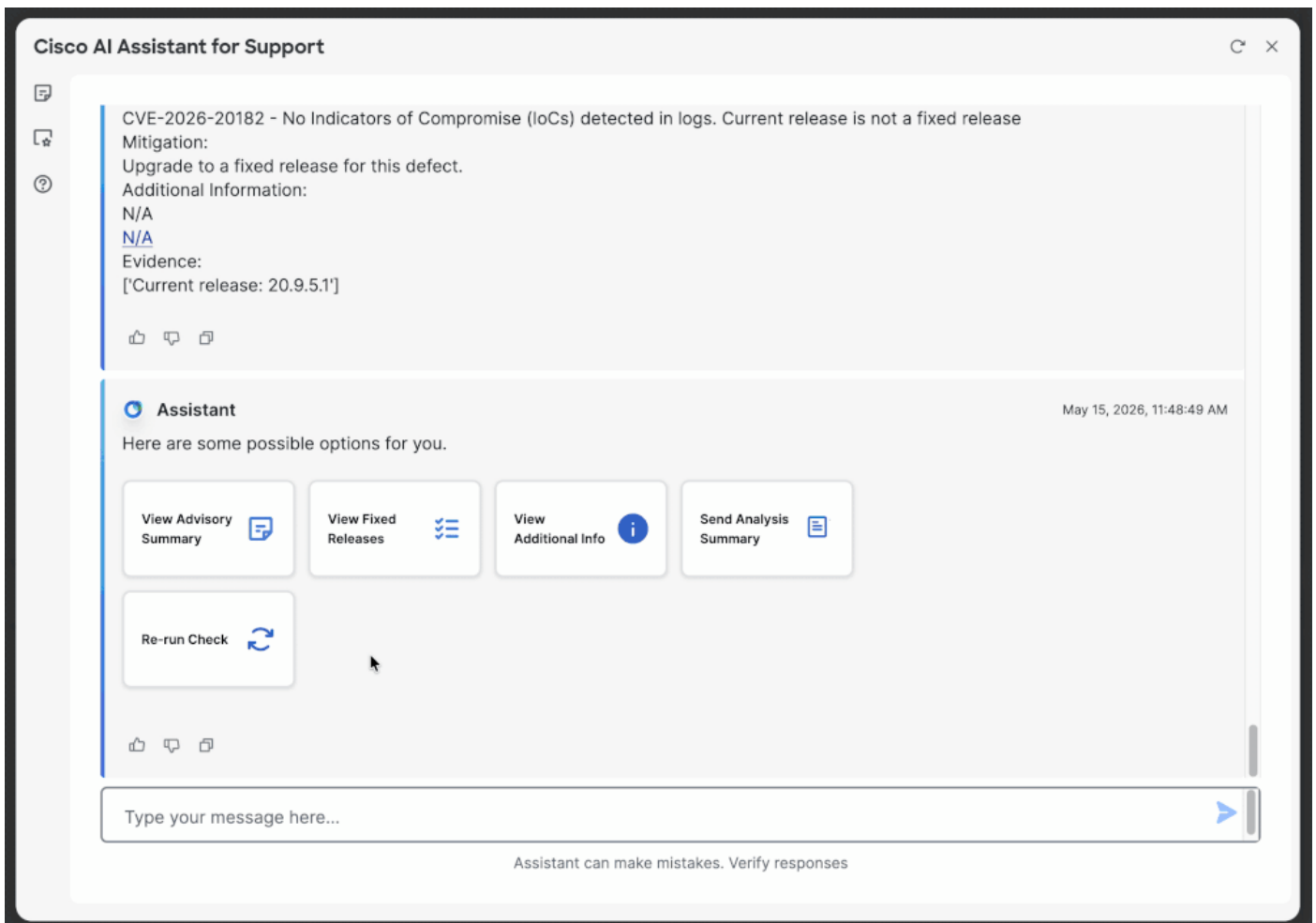
Veillez [ouvrir un dossier Cisco TAC](#) et télécharger le fichier admin-techs pour une révision manuelle supplémentaire.

Remarque : Si vous n'avez pas encore effectué la mise à niveau, veuillez procéder immédiatement à la mise à niveau vers une version contenant le correctif.



## Analyser un Admin-Tech supplémentaire

Pour analyser un autre admin-tech, cliquez sur "Re-run" et entrez l'ID de bogue Cisco applicable (par exemple, [CSCwt50498](#)) pour voir à nouveau la section de téléchargement. D'autres options incluent le défilement vers le haut et le clic sur "Vérifier <ID de bogue>" ou la saisie de l'ID de bogue dans la discussion.



## Options supplémentaires disponibles

Après l'analyse d'un admin-tech, ces options supplémentaires sont disponibles dans l'outil :

- Afficher le récapitulatif des conseils
  - Afficher les versions fixes
  - Afficher les informations supplémentaires
  - Envoyer le résumé des analyses
-

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.