

# Verifieer SD-WAN PSIRT met de Check Bug Application Tool

## Inhoud

---

[Inleiding](#)

[Vereisten](#)

[Admin-Tech Generation-richtlijnen](#)

[Beperkingen](#)

[gebruik](#)

[Verifieer een Admin-Tech](#)

[Resultaten - geen indicatoren](#)

[Resultaten - indicatoren gevonden](#)

[Analyseer een extra admin-tech](#)

[Extra opties beschikbaar](#)

---

## Inleiding

In dit document wordt beschreven hoe u de Bug Application tool gebruikt om admin-tech bestanden te scannen op mogelijke indicatoren van compromis (IoC's) met betrekking tot SD-WAN Product Security Incident Response Team (PSIRT) CVE-2026-20182 [CSCwt50498](#)

## Vereisten

Voor [CSCwt50498](#) moet u een admin-tech van uw SD-WAN-besturingscomponenten genereren. De Controller (vSmart) admin-techs moeten één voor één worden gegenereerd.

De admin-techs van andere SD-WAN-besturingscomponenten kunnen in elke volgorde worden gegenereerd.

## Admin-Tech Generation-richtlijnen

Als u hulp nodig hebt bij het maken van deze bestanden, raadpleegt u dit document met de stappen voor het genereren van een admin-tech: [Hoe een Admin-Tech in een SD-WAN-omgeving te verzamelen](#).

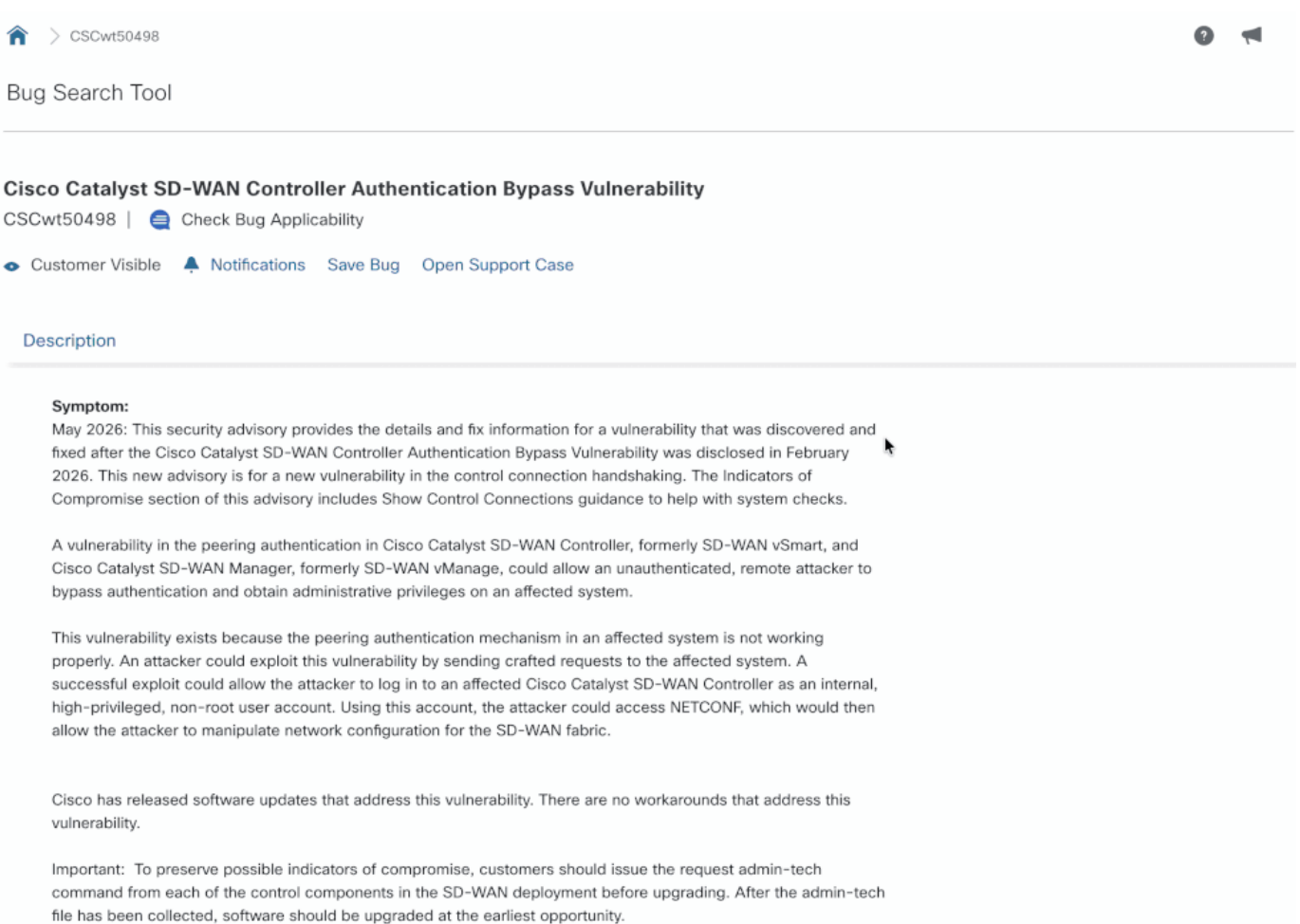
# Beperkingen

- De bestandsgrootte is momenteel beperkt tot 500 MB.
- Gelijktijdige bestandsverificatie wordt niet ondersteund. De tool kan meerdere bestanden verwerken, maar slechts één tegelijk.

## gebruik

### Verifieer een Admin-Tech

1. Ga naar de pagina Cisco Bug Search Tool voor de Cisco Bug ID die u wilt analyseren.
2. Klik onder de titel op de tekst of het pictogram "Controleer de toepasbaarheid van bugs". Er verschijnt een pop-upvenster.
3. Drop of selecteer het admin-tech bestand dat u wilt analyseren.



The screenshot shows the Cisco Bug Search Tool interface for bug CSCwt50498. The page title is "Bug Search Tool" and the bug title is "Cisco Catalyst SD-WAN Controller Authentication Bypass Vulnerability". The bug ID is CSCwt50498. There are navigation links for "Customer Visible", "Notifications", "Save Bug", and "Open Support Case". The "Description" section is expanded, showing the "Symptom" and "Description" of the vulnerability. The "Symptom" section states that the vulnerability was discovered in May 2026 and is related to the Cisco Catalyst SD-WAN Controller Authentication Bypass Vulnerability. The "Description" section explains that the 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. The page also mentions that Cisco has released software updates that address this vulnerability and that there are no workarounds that address this vulnerability. Finally, it states that it is important to preserve possible indicators of compromise by issuing the request admin-tech command from each of the control components in the SD-WAN deployment before upgrading.

Home > 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.

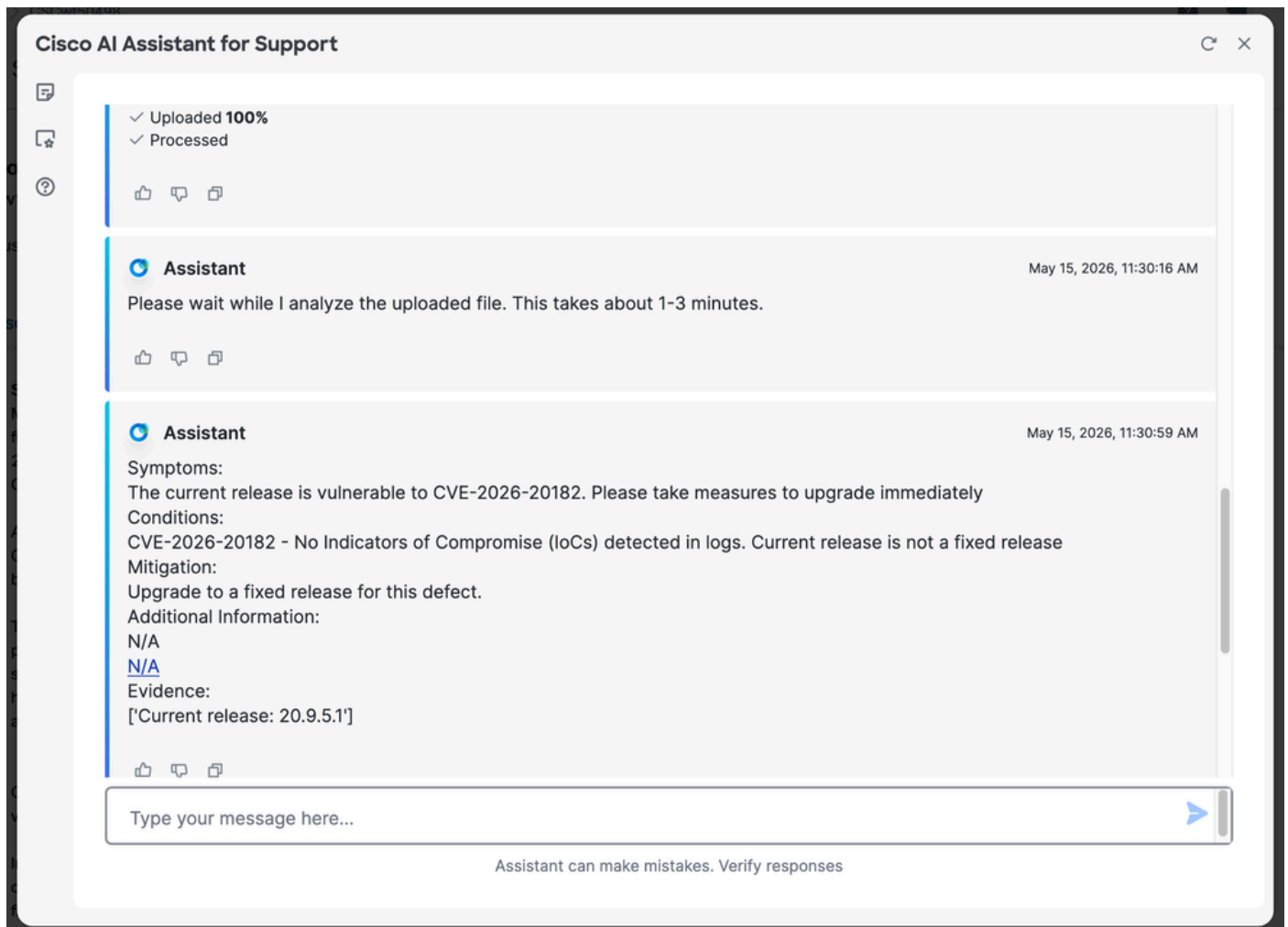
Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.

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.

## Resultaten - geen indicatoren

Als er geen indicatoren worden gevonden, wordt een bericht vergelijkbaar met "CVE-2026-20182 - No Indicators of Compromise (IoC's) Detected in logs. Huidige release is geen vaste release" verschijnt. Het bericht verwijst naar de specifieke Bug ID die wordt geanalyseerd.

Opmerking: als u nog geen upgrade hebt uitgevoerd, gaat u verder en upgradet u onmiddellijk naar een release met de oplossing.



## Resultaten - indicatoren gevonden

Als de tool indicatoren vindt, verschijnt het bericht "Potential Indicators of Compromise (IoC's) Detected".

Open [een Cisco TAC-case](#) en upload de admin-techs voor verdere handmatige beoordeling.

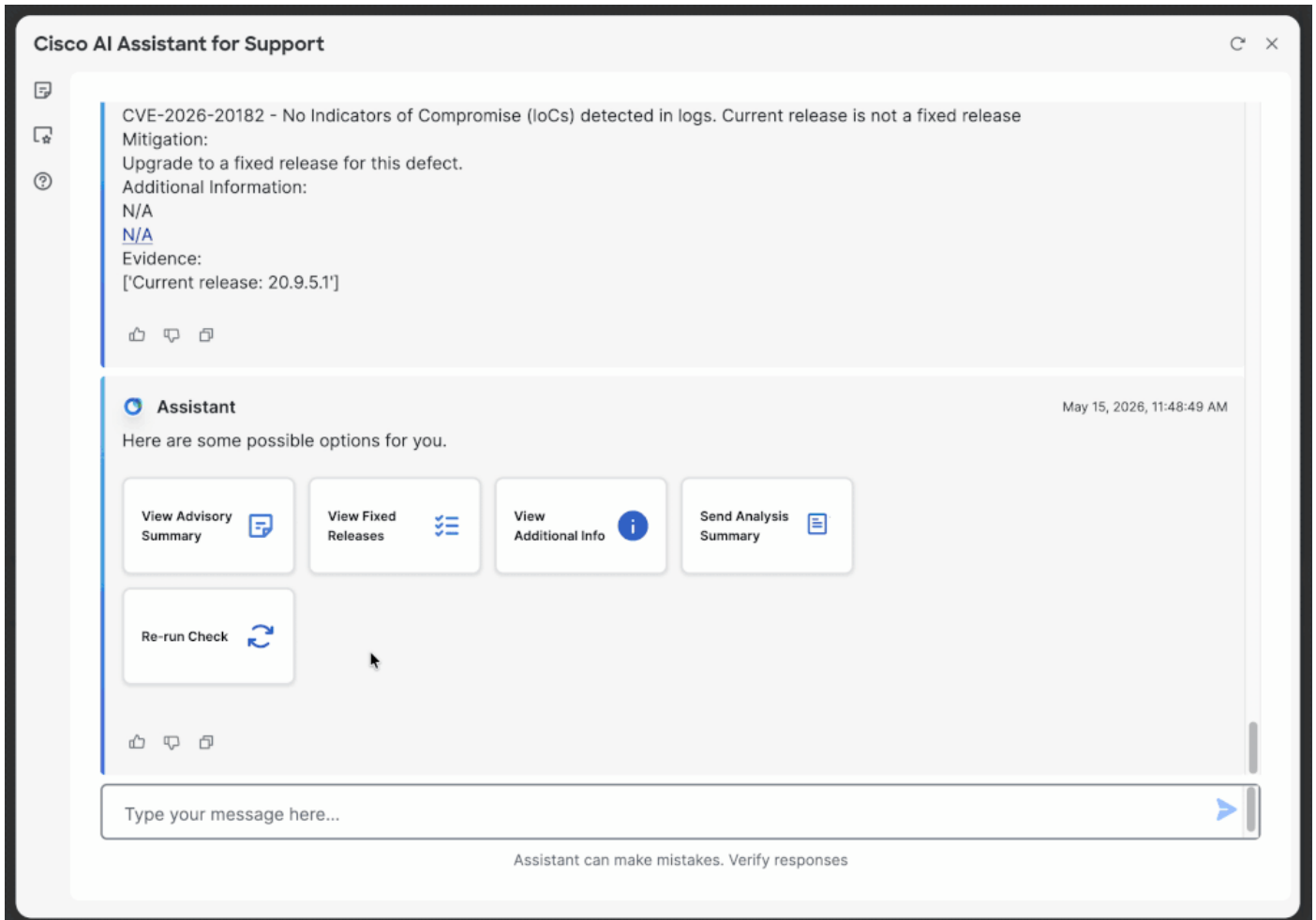
Opmerking: als u nog geen upgrade hebt uitgevoerd, gaat u verder en upgradet u onmiddellijk

naar een release met de oplossing.



## Analyseer een extra admin-tech

Om een andere admin-tech te analyseren, klikt u op "Opnieuw uitvoeren" en voert u de toepasselijke Cisco Bug ID in (bijv. [CSCwt50498](#)) om het uploadgedeelte opnieuw te bekijken. Andere opties zijn scrollen en klikken op "Controleer <Bug ID>" of het typen van de bug-ID in de chat.



## Extra opties beschikbaar

Na het analyseren van een admin-tech, zijn deze extra opties beschikbaar in de tool:

- Adviesamenvatting bekijken
  - Vaste releases bekijken
  - Extra informatie bekijken
  - Analyseoverzicht verzenden
-

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.