

Verifique el PSIRT de SD-WAN con la herramienta Check Bug Applicability

Contenido

[Introducción](#)

[Requirements](#)

[Directrices de generación de tecnología de administración](#)

[Limitaciones](#)

[Utilización](#)

[Verificar una tecnología de administración](#)

[Resultados: sin indicadores](#)

[Resultados - Indicadores encontrados](#)

[Análisis de una tecnología de administración adicional](#)

[Opciones adicionales disponibles](#)

Introducción

Este documento describe cómo utilizar la herramienta Bug Applicability para analizar los archivos admin-tech en busca de posibles indicadores de compromiso (IoC) relacionados con el equipo de respuesta ante incidentes de seguridad de productos (PSIRT) SD-WAN CVE-2026-20182 [CSCwt50498](#)

Requirements

Para [CSCwt50498](#), debe generar un admin-tech de sus componentes de control SD-WAN. Los controladores (vSmart) admin-techs deben generarse de uno en uno.

Los técnicos de administración de otros componentes de control de SD-WAN se pueden generar en cualquier orden.

Directrices de generación de tecnología de administración

Si necesita ayuda para crear estos archivos, consulte este documento que proporciona los pasos para generar un admin-tech: [Cómo recopilar una Admin-Tech en un entorno SD-WAN](#).

Limitaciones

- El tamaño del archivo está actualmente limitado a 500 MB.
- No se admite la verificación simultánea de archivos. La herramienta puede procesar varios archivos, pero sólo uno a la vez.

Utilización

Verificar una tecnología de administración

1. Vaya a la página de la herramienta de búsqueda de errores de Cisco para la ID de error de Cisco que desea analizar.
2. Debajo del título, haga clic en el texto o icono "Check Bug Applicability". Aparecerá una ventana emergente.
3. Quite o seleccione el archivo admin-tech que desee analizar.

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.

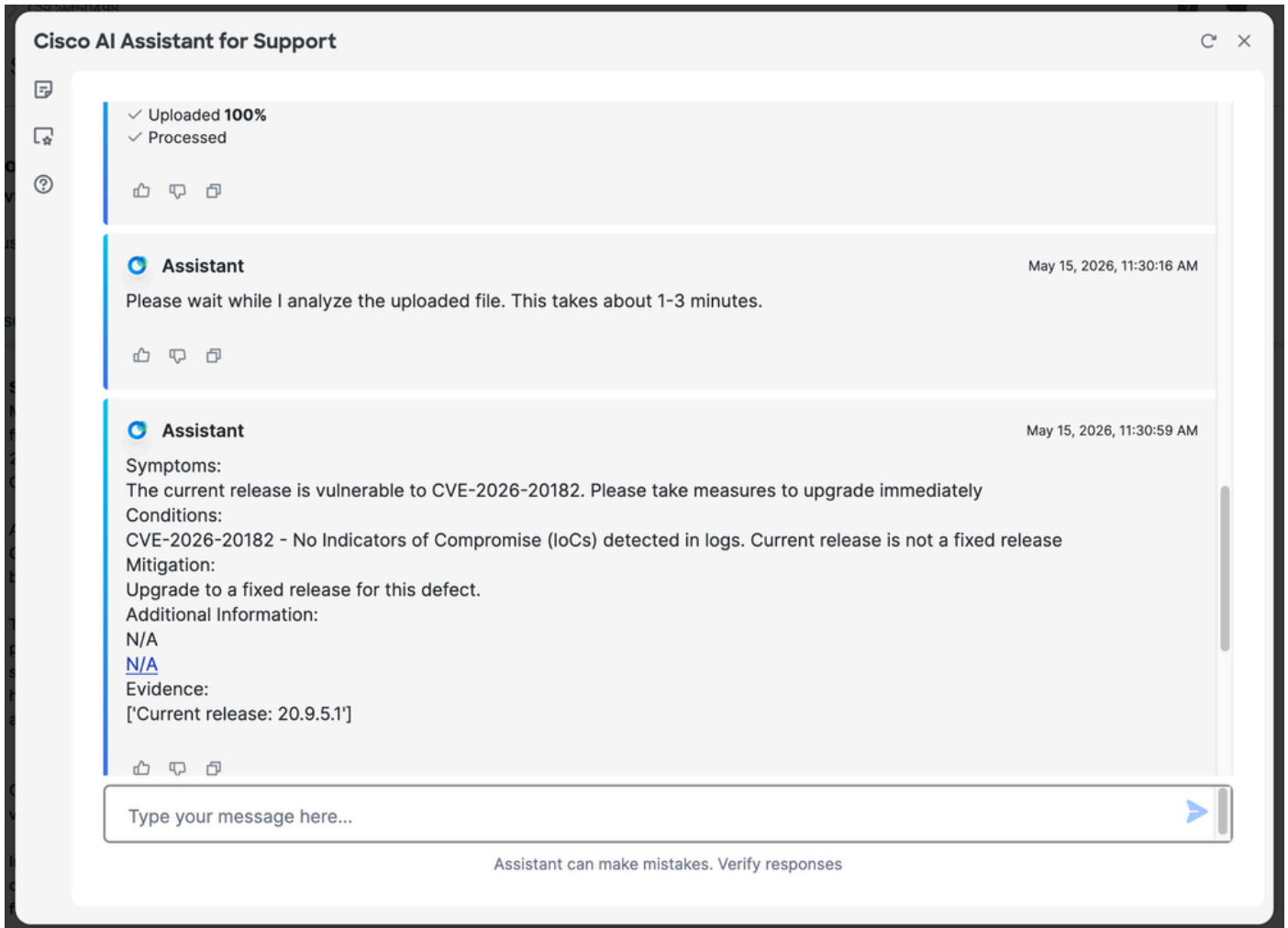
Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.

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.

Resultados: sin indicadores

Si no se encuentra ningún indicador, aparece un mensaje similar a "CVE-2026-20182 - No Indicators of Compromise (IoC) detected in logs. La versión actual no es una versión fija" aparece. El mensaje hará referencia al ID de bug específico que se está analizando.

Nota: Si aún no ha actualizado, continúe y actualice inmediatamente a una versión que contenga la corrección.



Resultados - Indicadores encontrados

Si la herramienta encuentra indicadores, aparecerá el mensaje "Potential Indicators of Compromise (IoC) Detected" (Posibles indicadores de compromiso [IoC] detectados).

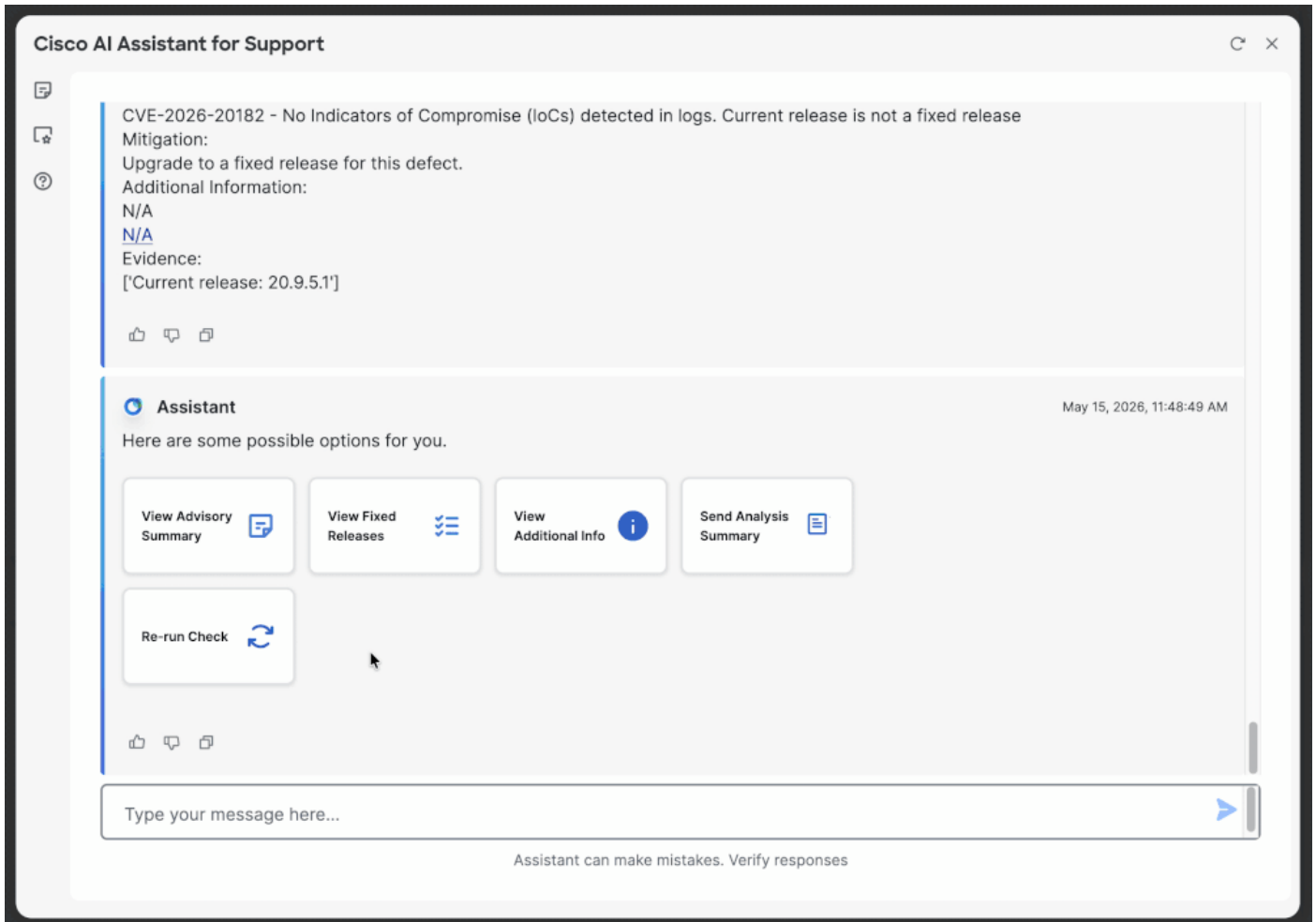
Abra [un caso de Cisco TAC](#) y cargue los técnicos administrativos para una revisión manual adicional.

Nota: Si aún no ha actualizado, continúe y actualice inmediatamente a una versión que contenga la corrección.



Análisis de una tecnología de administración adicional

Para analizar otro técnico de administración, haga clic en "Volver a ejecutar" e introduzca la ID de error de Cisco correspondiente (por ejemplo, [CSCwt50498](#)) para volver a ver la sección de carga. Otras opciones incluyen desplazarse hacia arriba y hacer clic en "Check <Bug ID>" o escribir el ID de bug en el chat.



Opciones adicionales disponibles

Después de analizar un técnico de administración, estas opciones adicionales están disponibles en la herramienta:

- Ver resumen de asesoramiento
 - Ver versiones fijas
 - Ver información adicional
 - Enviar resumen de análisis
-

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).