

ةادأ مادختساب SD-WAN PSIRT نم ققحت عاطخالا قيبطت نم ققحتلا

تايوتحمل

[ةمدقمل](#)

[تابلطتمل](#)

[Admin-Tech عاشن ا تاداشرا](#)

[دويقل](#)

[عافتنال](#)

[Admin-Tech نم ققحتلا](#)

[تارش فم دجوت ال - جئاتنلا](#)

[اهل ع روث عل امت يتللا تارش فملا - جئاتنلا](#)

[ةيفاضال Admin-tech ليلحت](#)

[قر فوملا ةيفاضال ا تارايل](#)

ةمدقمل

ةصاخلا admin-tech تافل م حسمل أطخالا قيبطت ةادأ مادختسا ةيفي ك دن تسملا اذه حضوي
تاجت نم نام ا ثداوحت ةباجت سالال قيرفب ةقلعتملا ةلمتحملا (IoCS) طسولا لولحلل تارش فمب
SD-WAN (PSIRT) CVE-2026-20182 [CSCwt50498](#)

تابلطتمل

SD-WAN يف مكحتلا تانوكمل admin ةينقت عاشن ا كيلع بجي [CSCwt50498](#) ةبسنلاب
ةرم لك يف ةدحاو (vSmart) مكحتلا ةدحول Admin-techs عاشن ا بجي. ك ةصاخلا

ببترت ي أب ىرخال SD-WAN يف مكحتلا تانوكمل Admin-techs عاشن ا نكمي.

Admin-Tech عاشن ا تاداشرا

يذلا دن تسملا اذه ىل ا عوجرلا ىجر يف ، تافل ملا هذه عاشن ا يف ةدعاسم ىل ا ةجاحب تنك اذ
SD-[ئيب يف ةيرادا ةينقت عيمجت ةيفي ك](#): ةرادا ةينقت عاشن ا ةمزاللا تاوطخال رفوي
[WAN](#).

دويقلا

- تبا باغيم 500 يل ع ايلاح فلملا مچ رصتقي
- دحاو نكل، ددعتم تافلما ةجلالعم ةادلل نكمي. موعدم ريغ نمازتملا فلملا نم ققحتلا ةرملك يف طقف

عافتال

Admin-Tech نم ققحتلا

1. يذلا Cisco نم ءاطخال فرعمب ءصاخلا Cisco نم ءاطخال نع شحبالا ءادأ ءحفص يل لقتنا هليحت ديرت
2. رهظت. "أطخال قيبطت ءينالما نم ققحت ءنوقيال وأ صنلا قوف رقنا، ناوئعلا تحت ءقثب نم ءذفان
3. هديحت وأ هليحت ديرت يذلا admin-tech فلم تالفاب مق

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.

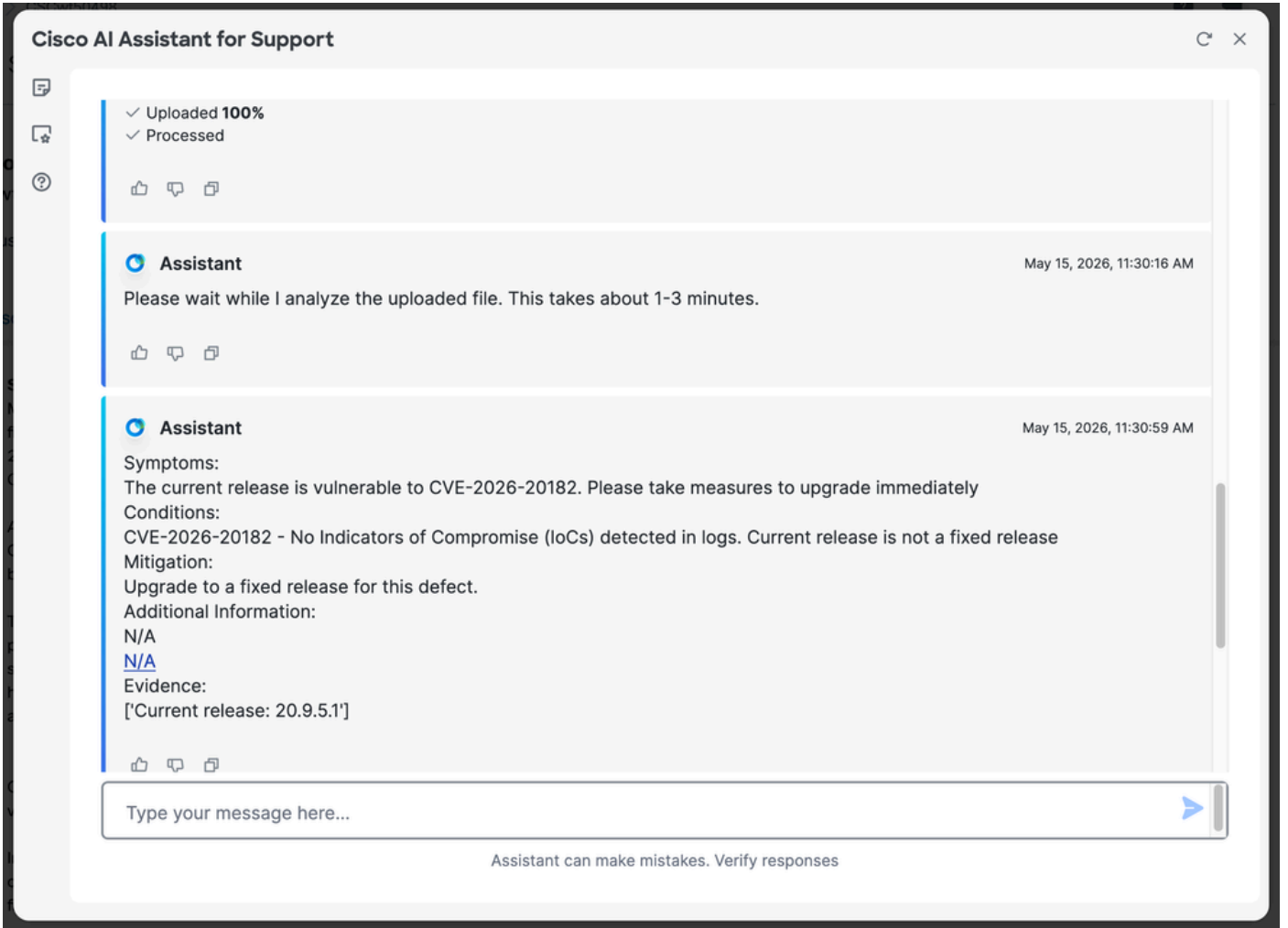
Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.

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.

تارشم دجوت ال - جئاتنل

دجوت ال - CVE-2026-20182 ل ةلثامم ةلاسرفاشتكام تي، تارشم يلع روثعلا متي مل اذا ريشت. "تبات رادصا سيل ليلاحال رادصا رهظي. تالجالا ي (IOS) ةيقي فوت تارشم هليلحت متي يذلا ددحمالا اطلخال فرعم ل ةلاسرلا

ل روفلا يلع ةيقرتلل او ةعباتملا يجرىف، دعب ةيقرتلل اب تمق دق نكت مل اذا: ةظحالم حالصا ليلع يوتحي رادصا



اهي لع روثةعلا م ت يةتلا تارشؤملا - جئاتنلا

(IoCS) قفاوتلل ةلمتحم تارشؤم ةلاسرلا رهظت ، تارشؤم يلع ةادألا ترتع اذا

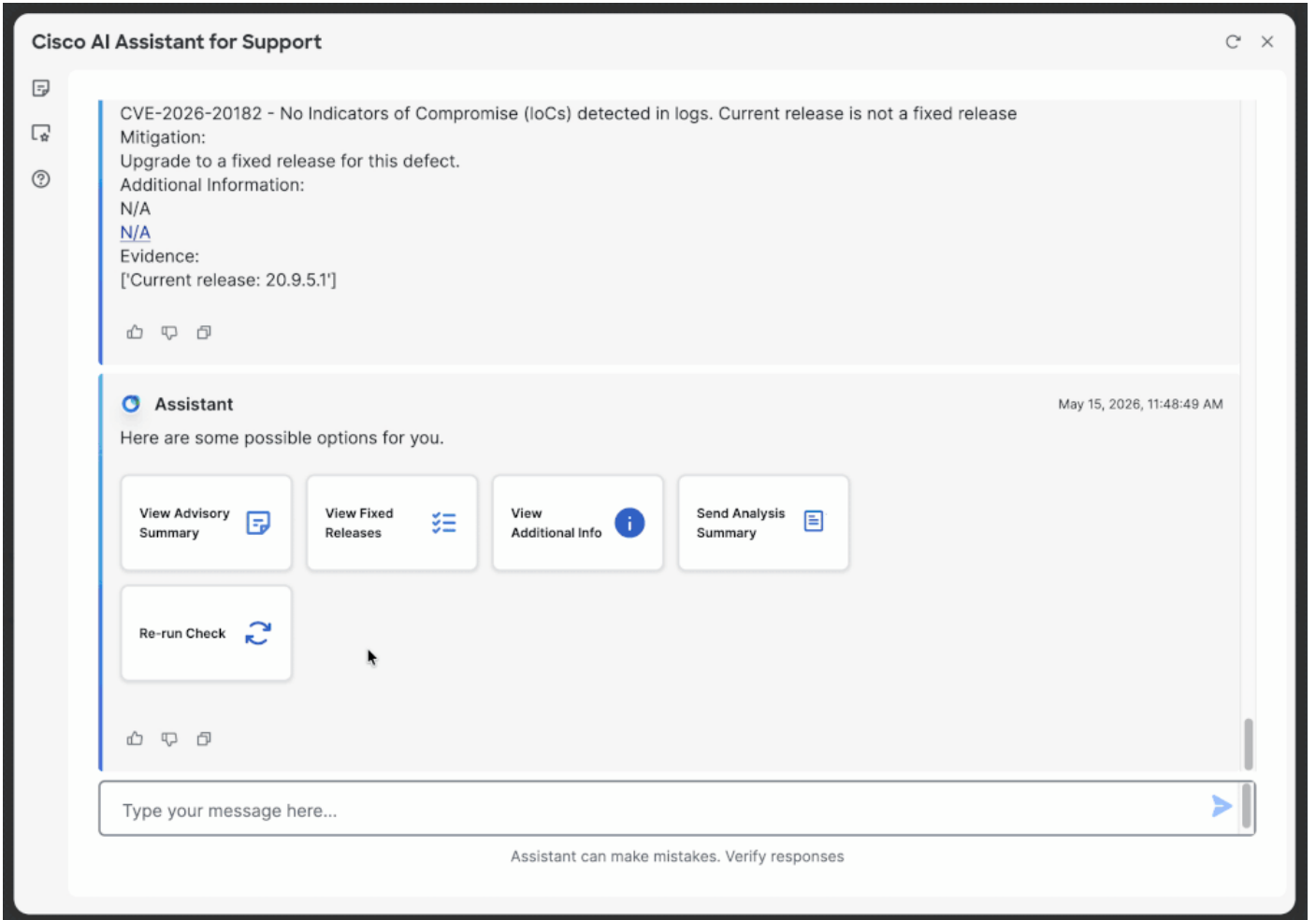
ةيوديلا ةعجارملا نم ديزملا admin-techs ليحمحتو [Cisco TAC](#) ةلاحتف ءاجر

ىلإ روفلا يلع ةيقرتلاو ةعباتملا يجري ف ، دعب ةيقرتلاب تمق دق نكت مل اذا : ةظحالم
جالصإلا يلع يوتحي رادصا



ةيفاضإل Admin-tech ليلحت

لباقولءاطخألءيحصتفرعملخدأو"ليغشالءءاعإ"قوفرقنا، admin-tech رخآ ليلحتل ةرم ليلحتال مسق لعلالطالل (CSCwt50498، لاثمال ليلبس لعل) Cisco نم قيبطلل وأ"أطخل فرعم" نم ققحتلال قوف رقلل اولعل ريرمئل رخألل اارايخل نمضتت. رخآ ةثءامل يف أطخل فرعم ةباتك.



ةرفوت ملة ةف اضاإل اارايأل

ةادال ةف ةف اضاإل اارايأل هذة رفوت ،ةرادال ةف نقت لةلحت دعب

- ةراشتسال صأل ملة اضرع
- ةتبال اارادصل اضرع
- ةف اضاإل اامولعمل اضرع
- لةلحتل صأل ملة لاسرا

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا ذه Cisco ت مچرت
م ل ا ل ا ا ن ا ع مچ ي ف ن ي م دخت س م ل ل م عد ي و ت ح م م ي دقت ل ة ي ر ش ب ل و
ا م ك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ا د ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا هذه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا