



NCSC-2026-0071

Kwetsbaarheden verholpen in Cisco Catalyst SD-WAN Manager

NCSC Advisory

PRIORITEIT: HOOG

Gepubliceerd op: 25-02-2026

TLP:WHITE

Toegestane verspreiding van TLP:WHITE

(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

Cisco heeft meerdere kwetsbaarheden verholpen in de Cisco Catalyst SD-WAN Manager.

Duiding

De kwetsbaarheden bevinden zich in de peering authenticatiemechanismen van de Cisco Catalyst SD-WAN Controller en Manager producten. Deze kwetsbaarheden stellen een niet-geauthenticeerde externe aanvaller in staat om het authenticatieproces te omzeilen, waardoor administratieve privileges op de getroffen systemen kunnen worden verkregen. Daarnaast kunnen aanvallers root-level privileges verkrijgen, wat kan leiden tot ongeautoriseerde toegang tot gevoelige informatie en de mogelijkheid om willekeurige bestanden te overschrijven, wat kan resulteren in verdere exploitatie of systeeminstabiliteit.

De meest ernstige kwetsbaarheid, met kenmerk CVE-2026-20127, kan door een ongeauthenticeerde kwaadwillende worden misbruikt om op afstand willekeurige code uit te voeren met hoge administratieve rechten. Cisco geeft aan dat actief misbruik van deze kwetsbaarheid bekend is.

Na misbruik van deze kwetsbaarheid zou de kwaadwillende de kwetsbaarheid met kenmerk CVE-2022-20775 gebruiken om de rechten te escaleren tot root. Dit doet de actor door het systeem te downgraden naar een versie waarin CVE-2022-20775 niet verholpen is, de rechten middels deze kwetsbaarheid te verhogen naar root en vervolgens het systeem weer terug te zetten in de oorspronkelijke versie.

Het NCSC verwacht op korte termijn een publieke PoC en grootschalige pogingen tot misbruik van CVE-2026-20127. Het NCSC adviseert met klem de update zo spoedig mogelijk te installeren.

Oplossingen

Cisco heeft updates uitgebracht om de kwetsbaarheden te verhelpen. In een blog geeft Talos informatie over het bekende misbruik en is er een validatie checklist beschikbaar gesteld met uitleg hoe deze kan worden toegepast. Zie bijgevoegde referenties voor meer informatie.

Referenties

- <https://blog.talosintelligence.com/uat-8616-sd-wan>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-authbp-qwCX8D4v>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa-EHchtZk>

Kwetsbaarheden

CVE	CVSS Score
> CVE-2026-20122	
> CVE-2026-20126	
> CVE-2026-20127	
> CVE-2026-20128	
> CVE-2026-20129	
> CVE-2026-20133	

CWE's

CWE	Beschrijving
> CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
> CWE-257	Storing Passwords in a Recoverable Format
> CWE-287	Improper Authentication
> CWE-648	Incorrect Use of Privileged APIs

Getroffen producten

Cisco
Catalyst SD-WAN Manager
Cisco Catalyst SD- WAN

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.