Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0071

Kwetsbaarheden verholpen in Cisco Catalyst SD-WAN Manager

NCSC Advisory

PRIORITEIT: HOOG

Gepubliceerd op: 06-03-2026
Revisie: 1.0.2

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

Update Revisie 2

Inmiddels is Proof-of-Concept-Code (PoC) verschenen die de kwetsbaarheid aantoont.

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.

Er is publieke Proof-of-Concept-code (PoC) verschenen die de kwetsbaarheid met kenmerk CVE-2026-20127 aantoont en mogelijk misbruikt. De kans op grootschalig misbruik neemt hierdoor toe en het NCSC verwacht een significante toename in scan- en misbruikverkeer. Het NCSC adviseert met klem de update zo spoedig mogelijk te installeren.

Ook van de kwetsbaarheden met kenmerk CVE-2026-20122 en CVE-2026-20128 meldt Cisco berichten te ontvangen dat deze actief worden misbruikt. Voor deze kwetsbaarheden is (nog) geen publieke Proof-of-Concept-code of exploit beschikbaar.

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	5.4 MEDIUM
CVE-2026-20126	8.8 HIGH
CVE-2026-20127	10.0 CRITICAL
CVE-2026-20128	7.5 HIGH
CVE-2026-20129	9.8 CRITICAL
CVE-2026-20133	6.5 MEDIUM

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