



NCSC-2026-0157

Kwetsbaarheden verholpen in Cisco Catalyst SD-WAN Controller en Manager

NCSC Advisory

PRIORITEIT: HOOG

Gepubliceerd op: 15-05-2026

Revisie: 1.0.1

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 1

CVE-2026-20209, CVE-2026-20210, CVE-2026-20224 toegevoegd.

Feiten

Cisco heeft een kwetsbaarheden verholpen in de Catalyst SD-WAN Controller en Manager producten.

Duiding

Cisco heeft 4 kwetsbaarheden verholpen in de Catalyst SD-WAN Controller en Manager producten. De kwetsbaarheden betreffen XXE-injectie, privilege-escalatie en authentication bypass. De authentication bypass kwetsbaarheid bevindt zich in het peering authenticatiemechanisme, waardoor niet-geauthenticeerde externe aanvallers verhoogde rechten kunnen verkrijgen. Hierdoor kunnen zij netwerkconfiguraties manipuleren en mogelijk netwerkkoperaties verstoren. Met name SD-WAN controllers die poorten via publieke netwerken bereikbaar hebben lopen een verhoogd risico op misbruik.

Cisco meldt bekend te zijn met berichten dat de authentication bypass kwetsbaarheid beperkt en gericht is misbruikt. De verwachting van het NCSC is dat op korte termijn een toename in scan- en misbruikverkeer zal plaatsvinden.

Oplossingen

Cisco heeft updates uitgebracht om de kwetsbaarheid te verhelpen. Ook heeft Cisco Indicators of Compromise (IoC's) beschikbaar gesteld om eventueel misbruik te detecteren. Zie bijgevoegde referenties voor meer informatie.

Dreigingsinformatie

Customers are encouraged to audit the auth.log file, located at /var/log/auth.log, for entries that are related to Accepted publickey for vmanage-admin from unknown or unauthorized IP addresses, as shown in the following example:

```
2026-02-10T22:51:36+00:00 vm sshd[804]: Accepted publickey for vmanage-admin from port [REDACTED PORT] ssh2: RSA SHA256:[REDACTED KEY]
```

Customers must check the IP address in the auth.log log file against the configured System IPs that are listed in the Cisco Catalyst SD-WAN Manager web UI in the WebUI > Devices > System IP column.

Referenties

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-mltvnps2-JxpWm7R>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa2-v69WY2SW>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2026-20209	5.4 MEDIUM
➤ CVE-2026-20224	8.6 HIGH
➤ CVE-2026-20210	5.4 MEDIUM
➤ CVE-2026-20182	10.0 CRITICAL

CWE's

CWE	Beschrijving
➤ CWE-287	Improper Authentication

Getroffen producten

Cisco
Catalyst SD-WAN
Catalyst SD-WAN Manager

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.