Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

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 netwerkoperaties 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