Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0277

Kwetsbaarheden verholpen in Cisco Catalyst SD-WAN

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 06-08-2026

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 Cisco Catalyst SD-WAN.

Duiding

De gevonden problemen betreffen onder andere onjuiste inputvalidatie, onjuiste toegangscontrole, onjuiste linkresolutie voorafgaand aan bestandsaccess en het opslaan van gevoelige informatie in cleartext. Door deze kwetsbaarheden kan de software mogelijk onbedoeld gedrag vertonen bij het verwerken van invoer, het controleren van toegangsrechten, het openen van bestanden, en het beschermen van gevoelige data.

Oplossingen

Cisco heeft updates uitgebracht. Zie bijgevoegde referenties voor meer informatie.

Referenties

› https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-sdwan-faLcR3K

Kwetsbaarheden

CVE	CVSS Score
› CVE-2026-20303	9.9 CRITICAL
› CVE-2026-20304	9.9 CRITICAL
› CVE-2026-20310	9.1 CRITICAL
› CVE-2026-20312	8.8 HIGH
› CVE-2026-20313	7.7 HIGH

CWE's

CWE	Beschrijving
› CWE-20	Improper Input Validation

CWE-59	Improper Link Resolution Before File Access ('Link Following')
CWE-284	Improper Access Control
CWE-312	Cleartext Storage of Sensitive Information
CWE-1284	Improper Validation of Specified Quantity in Input

Getroffen producten

Cisco
Catalyst SD-WAN Manager
Cisco Catalyst SD-WAN Controller

Disclaimer