Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0270

Kwetsbaarheden verholpen in Cisco NX-OS Software

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 28-08-2025

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 kwetsbaarheden verholpen in Cisco NX-OS Software (Specifiek voor Nexus 3000 en 9000 Series Switches).

Duiding

De kwetsbaarheden bevinden zich in verschillende functies van de Cisco NX-OS Software. Een kwetsbaarheid in de command-line interface (CLI) stelt geauthenticeerde lokale kwaadwillenden in staat om command injection-aanvallen uit te voeren, wat kan leiden tot ongeautoriseerde toegang en manipulatie van systeembestanden. Een andere kwetsbaarheid in de IS-IS-functie kan door een niet-geauthenticeerde, aangrenzende aanvaller worden misbruikt, wat kan resulteren in een denial-of-service (DoS) situatie. Daarnaast kan een kwetsbaarheid in de loggingfunctie leiden tot ongeautoriseerde toegang tot gevoelige informatie. Tot slot kan de PIM6-functie worden gecompromitteerd door laaggeprivilegieerde geauthenticeerde externe kwaadwillenden, wat ook kan leiden tot een DoS-conditie.

Oplossingen

Cisco heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-n39k-isis-dos-JhJA8Rfx
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmdinj-qhNze5Ss
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-infodis-TEcTYSFG
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxospc-pim6-vG4jFPh

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-20292	4.4 MEDIUM
CVE-2025-20241	7.4 HIGH

CVE-2025-20290	**5.5 MEDIUM**
CVE-2025-20262	**5.0 MEDIUM**

CWE's

CWE	Beschrijving
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-476	NULL Pointer Dereference
CWE-733	Compiler Optimization Removal or Modification of Security-critical Code

Getroffen producten

Cisco
Cisco Nexus 3000 Series Switches
Cisco Nexus 9000 Series Switches

Disclaimer