Nationaal Cyber Security Centrum
*Ministerie van Justitie en Veiligheid*

# NCSC-2025-0287

## Kwetsbaarheden verholpen in Cisco NX-OS Software

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 11-09-2025

**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 voor Nexus 3000 en 9000 Series Switches.

## Duiding

De kwetsbaarheden bevinden zich in verschillende functies van de Cisco NX-OS Software, waaronder IS-IS, PIM6, logging, command-line interface (CLI), en de REST API van de Nexus Dashboard. Deze kwetsbaarheden kunnen worden misbruikt door zowel geauthenticeerde als niet-geauthenticeerde aanvallers om Denial-of-Service (DoS) te veroorzaken, ongeautoriseerde toegang tot gevoelige informatie te verkrijgen, en zelfs rootprivileges op de apparaten te verkrijgen. De ernst van deze kwetsbaarheden vereist onmiddellijke aandacht van beveiligingsbeheerders die deze apparaten beheren.

## 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-nd-ptrs-XU2Fm2Wb
› https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nshs-urapi-gJuBVFpu

› 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-2025-20241 | 7.4 HIGH |
| › CVE-2025-20262 | 5.0 MEDIUM |

| | |
|---|---|
| CVE-2025-20290 | **5.5 MEDIUM** |
| CVE-2025-20292 | **4.4 MEDIUM** |
| CVE-2025-20344 | |
| CVE-2025-20347 | **5.4 MEDIUM** |
| CVE-2025-20348 | **5.0 MEDIUM** |

## CWE's

| CWE | Beschrijving |
|---|---|
| CWE-22 | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') |
| 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-201 | Insertion of Sensitive Information Into Sent Data |
| CWE-476 | NULL Pointer Dereference |
| CWE-693 | Protection Mechanism Failure |
| CWE-733 | Compiler Optimization Removal or Modification of Security-critical Code |

## Getroffen producten

| **Cisco** |
|---|
| Cisco Data Center Network Manager |
| Cisco MDS 9000 Multilayer Directors and Fabric Switches |
| Cisco NX-OS Software |

| |
|---|
| Cisco NX-OS System Software in ACI Mode |
| Cisco Nexus 1000V Series Switches |
| Cisco Nexus 3000 Series Switches |
| Cisco Nexus 5000 Series Switches |
| Cisco Nexus 7000 Series Switches |
| Cisco Nexus 9000 Series Switches |
| Cisco Nexus Dashboard |
| Cisco Unified Computing System (Managed) |
| NX-OS |
| Nexus |
| Nexus Dashboard |
| Nexus Dashboard Fabric Controller |
| Unified Computing System (UCS) |
| nx-os_aci_mode |

## Disclaimer