



# 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](http://www.first.org/tlp)).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op [info@ncsc.nl](mailto: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-ptns-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
> CVE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
> CVE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
> CVE-200	Exposure of Sensitive Information to an Unauthorized Actor
> CVE-201	Insertion of Sensitive Information Into Sent Data
> CVE-476	NULL Pointer Dereference
> CVE-693	Protection Mechanism Failure
> CVE-733	Compiler Optimization Removal or Modification of Security-critical Code

## Getroffen producten

<b>Cisco</b>
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

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.