



# 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](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 (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

<a href="#">&gt; CVE-2025-20290</a>	<b>5.5 MEDIUM</b>
<a href="#">&gt; CVE-2025-20262</a>	<b>5.0 MEDIUM</b>

## CWE's

CWE	Beschrijving
<a href="#">&gt; CWE-78</a>	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
<a href="#">&gt; CWE-200</a>	Exposure of Sensitive Information to an Unauthorized Actor
<a href="#">&gt; CWE-476</a>	NULL Pointer Dereference
<a href="#">&gt; CWE-733</a>	Compiler Optimization Removal or Modification of Security-critical Code

## Getroffen producten

Cisco
Cisco Nexus 3000 Series Switches
Cisco Nexus 9000 Series Switches

## 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.