



Advisory NCSC-2026-0406

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Cisco NX-OS Software

Publicatiedatum: 08-10-2026

Toegestane verspreiding: TLP:WHITE
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (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.

Reacties zijn welkom op info@ncsc.nl.

Feiten

Cisco heeft meerdere kwetsbaarheden verholpen in Cisco NX-OS Software.

Duiding

De kwetsbaarheden betreffen verschillende componenten van Cisco NX-OS Software.

- Een kwetsbaarheid in de Python interpreter maakt het mogelijk voor een geauthenticeerde lokale aanvaller met lage privileges om de Python sandbox te ontsnappen en willekeurige commando's op het onderliggende besturingssysteem uit te voeren.
- Een andere kwetsbaarheid in de NX-API feature laat ongeauthenticeerde externe aanvallers toe om via onvoldoende inputvalidatie van HTTP-verzoeken willekeurige code met rootrechten uit te voeren of een denial of service te veroorzaken.
- Daarnaast kunnen ongeauthenticeerde externe aanvallers door het ontbreken van adequate rate limiting op bepaalde protocollen systeembronnen uitputten, wat leidt tot tijdelijke verstoringen in routing en control plane protocollen.
- Verder zijn er meerdere intern ontdekte kwetsbaarheden die betrekking hebben op improper neutralization (CWE-707), improper access control (CWE-284), improper input validation (CWE-20), out-of-bounds read (CWE-125), improper handling of exceptional conditions (CWE-703) en out-of-bounds write (CWE-787). Deze kwetsbaarheden kunnen leiden tot verschillende vormen van ongeautoriseerde toegang, systeeminstabiliteit of verstoring van de werking van het netwerkbesturingssysteem.

De kwetsbaarheden zijn geïdentificeerd tijdens interne beveiligingsreviews door het engineeringteam van Cisco en voor zover bekend is geen van de kwetsbaarheden actief misbruikt.

Oplossingen

Cisco heeft software hardening updates uitgebracht voor Cisco NX-OS Software om deze kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-nxosw1-cWzSbtR>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-napi-rce-r2shwu2j>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-notice-fBn58ELx>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-mppe-dhKZAFgb>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-nscpdos-SnderkC7>

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-20032	4.4 MEDIUM
CVE-2026-20173	5.8 MEDIUM
CVE-2026-76453	8.8 HIGH
CVE-2026-76455	9.8 CRITICAL
CVE-2026-76456	8.6 HIGH
CVE-2026-76457	8.6 HIGH
CVE-2026-76458	8.6 HIGH
CVE-2026-76459	8.8 HIGH
CVE-2026-76471	9.8 CRITICAL

CWE's

CWE	Beschrijving
CWE-122	Heap-based Buffer Overflow
CWE-125	Out-of-bounds Read
CWE-653	Improper Isolation or Compartmentalization
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-787	Out-of-bounds Write

Getroffen producten

Cisco
Cisco MDS 9000 Multilayer Directors and Fabric Switches
Cisco Nexus 3000 Series Switches
Cisco Nexus 7000 Series Switches
Cisco Nexus 9000 Series Switches
Cisco Unified Computing System (Managed)
NX-OS

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 or 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.