



NCSC-2026-0338

Kwetsbaarheden verholpen in Cisco Nexus 9000 Series, IOS XR Software en Secure Email

NCSC Security Advisory

Prioriteit: Normaal

Gepubliceerd op: 03-09-2026

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 Nexus 9000 Series Switches met Silicon One technologie, Cisco IOS XR Software en Cisco Secure Email.

Duiding

De ernstigste kwetsbaarheid betreft Nexus 9000-switches: als TCP 43210 of 43211 bereikbaar is, kan een aanvaller zonder authenticatie code met rootrechten uitvoeren en de switch laten herstarten. De IOS XR-kwetsbaarheden kunnen, afhankelijk van platform en configuratie, diverse beveiligingsfuncties ondermijnen. De Secure Email-kwetsbaarheden kunnen alleen bij een man-in-the-middlepositie en S/MIME-gebruik leiden tot het ontsleutelen van e-mail en het aanpassen van verkeer tussen e-mail gateways.

Oplossingen

Cisco heeft updates uitgebracht voor Cisco Nexus 9000 Series Switches, IOS XR Software en Secure Email om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-smime-disc-dzw4rEdY>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-iosxr-qg64NcM>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-n9k-s1-rce-EH8dEtr>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2026-20212	9.8 CRITICAL
➤ CVE-2026-20274	9.8 CRITICAL
➤ CVE-2026-20275	8.8 HIGH
➤ CVE-2026-20276	8.6 HIGH
➤ CVE-2026-20277	8.2 HIGH

> CVE-2026-20278	8.8 HIGH
> CVE-2026-20279	9.8 CRITICAL
> CVE-2026-20280	8.8 HIGH
> CVE-2026-20354	5.9 MEDIUM
> CVE-2026-20355	5.9 MEDIUM

CWE's

CWE	Beschrijving
> CWE-354	Improper Validation of Integrity Check Value
> CWE-1327	Binding to an Unrestricted IP Address

Getroffen producten

Cisco
AsyncOS
Cisco IOS XR
Cisco IOS XR Software
Cisco NX-OS Software
Cisco Nexus 9000 Series Switches
Cisco Secure Email
Nexus
Secure Email Gateway

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.