



NCSC-2026-0279

Kwetsbaarheden verholpen in Cisco IOS XE Software

NCSC Security Advisory

Prioriteit: Normaal

Gepubliceerd op: 07-08-2026

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 meerdere kwetsbaarheden verholpen in Cisco IOS XE Software.

Duiding

De kwetsbaarheden zijn intern ontdekt tijdens een uitgebreide beveiligingsreview van Cisco IOS XE Software. De geïdentificeerde problemen betreffen onder andere onjuiste toegangscontrole, onjuiste restricties bij geheugenbufferoperaties, onjuiste resourcecontrole, onjuiste berekeningen, onvoldoende control flow management, onjuiste neutralisatie van speciale elementen en onjuiste inputvalidatie. De kwetsbaarheden kunnen door een aanvaller worden misbruikt via de genoemde zwakheden in toegang, geheugenbeheer, resourcebeheer, berekeningen, control flow, neutralisatie van speciale elementen en inputvalidatie. De kwetsbaarheden zijn specifiek voor Cisco IOS XE Software.

Oplossingen

Cisco heeft software updates uitgebracht voor Cisco IOS XE Software om deze intern ontdekte kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

➤ <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-iosxe-V8NMuMZJ>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2026-20267	9.0 CRITICAL
➤ CVE-2026-20268	8.6 HIGH
➤ CVE-2026-20269	8.6 HIGH
➤ CVE-2026-20270	8.6 HIGH
➤ CVE-2026-20271	8.6 HIGH
➤ CVE-2026-20272	9.8 CRITICAL

> CVE-2026-20273

8.6 HIGH

CWE's

CWE	Beschrijving
> CWE-20	Improper Input Validation
> CWE-74	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')
> CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer
> CWE-284	Improper Access Control
> CWE-664	Improper Control of a Resource Through its Lifetime
> CWE-682	Incorrect Calculation
> CWE-691	Insufficient Control Flow Management

Getroffen producten

Cisco
Cisco IOS XE Software

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.