



Advisory NCSC-2026-0407

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Cisco License On-Prem

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 License On-Prem.

Duiding

De kwetsbaarheden bevinden zich in de webgebaseerde managementinterface en API-eindpunten van Cisco License On-Prem. Niet-geauthenticeerde aanvallers kunnen onder meer wachtwoorden resetten, bestanden schrijven of DoS-condities veroorzaken. Geauthenticeerde aanvallers met beheerdersrechten kunnen willekeurige commando's met rootrechten uitvoeren en via SQL-injectie toegang krijgen tot interne database-inhoud. Daarnaast zijn kwetsbaarheden vastgesteld rond authenticatie, cryptografische verificatie, credentialbescherming en code-injectie. De kwetsbaarheden kunnen gevolgen hebben voor de vertrouwelijkheid, integriteit en beschikbaarheid van het product.

De kwetsbaarheden bevinden zich in de webinterface en API van Cisco License On-Prem. Het is af te raden om dergelijke interfaces publiek toegankelijk te hebben. Maar ook op interne netwerken is het aan te raden dergelijke interfaces af te steunen in separate beheeromgevingen, of additionele maatregelen te nemen om ongeautoriseerde toegang zo veel mogelijk te beperken.

Oplossingen

Cisco heeft updates uitgebracht om de kwetsbaarheden in Cisco License On-Prem te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-ssm-Ph77wdhf>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ssm-access-nttb2dhE>

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-20328	9.1 CRITICAL
CVE-2026-76437	4.9 MEDIUM
CVE-2026-76452	4.9 MEDIUM
CVE-2026-76454	9.1 CRITICAL
CVE-2026-76480	9.8 CRITICAL
CVE-2026-76482	10.0 CRITICAL
CVE-2026-76483	9.1 CRITICAL
CVE-2026-76484	8.8 HIGH

CWE's

CWE	Beschrijving
CWE-23	Relative Path Traversal
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
CWE-862	Missing Authorization
CWE-94	Improper Control of Generation of Code ('Code Injection')
CWE-306	Missing Authentication for Critical Function
CWE-347	Improper Verification of Cryptographic Signature
CWE-522	Insufficiently Protected Credentials

Getroffen producten

Cisco

Cisco License On-Prem

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.