Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0323

Kwetsbaarheden verholpen in Cisco Secure Workload

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 21-08-2026

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 Secure Workload.

Duiding

De kwetsbaarheden betreffen onder andere improper neutralization of special elements (CWE-74), improper access control (CWE-284), improper authentication (CWE-287), improper input validation (CWE-20) en buffer management problemen (CWE-119). Deze kwetsbaarheden zijn intern ontdekt tijdens een uitgebreide security review door het engineering team van Cisco Secure Workload. Een aanvaller kan mogelijk misbruik maken van deze kwetsbaarheden afhankelijk van de specifieke aard van de fout, zoals het omzeilen van toegangscontroles, authenticatiefouten, of het veroorzaken van onjuiste verwerking van invoer. De kwetsbaarheden zijn opgelost door middel van software hardening updates.

Oplossingen

Cisco heeft software hardening updates uitgebracht om de kwetsbaarheden in Cisco Secure Workload te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

› https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-csw1-shSvndWP

Kwetsbaarheden

CVE	CVSS Score
› CVE-2026-20231	9.9 CRITICAL
› CVE-2026-20315	10.0 CRITICAL
› CVE-2026-20317	10.0 CRITICAL
› CVE-2026-20318	9.6 CRITICAL
› CVE-2026-20319	7.5 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-287	Improper Authentication

Getroffen producten

Cisco
Secure Workload

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.