



Advisory NCSC-2026-0429

PRIORITEIT: HOOG

Kwetsbaarheid verholpen in Cisco Secure Email Gateway

Publicatiedatum: 14-10-2026

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 een kwetsbaarheid verholpen in Cisco Secure Email Gateway, specifiek in de Advanced Malware Protection feature.

Duiding

De kwetsbaarheid bevindt zich in de wijze waarop de Advanced Malware Protection feature e-mailbijlagen verwerkt wanneer de file reputation service is ingeschakeld. Een niet-geauthenticeerde externe aanvaller kan hierdoor willekeurige bestanden schrijven naar het onderliggende besturingssysteem. Misbruik van deze kwetsbaarheid kan leiden tot het uitvoeren van commando's met rootrechten, wat de systeemintegriteit beïnvloedt.

Cisco meldt bekend te zijn met actief misbruik en heeft Indicators of Compromise en uitgebreide achtergrondinformatie gedeeld.

Op dit moment is (nog) geen Proof-of-Concept-code (PoC) of exploitcode bekend, maar door de aard van de kwetsbaarheid is het aannemelijk dat op korte termijn een PoC of exploit publiek beschikbaar komt. Het NCSC verwacht daarom een toename in scanverkeer en pogingen tot misbruik.

Oplossingen

Cisco heeft updates uitgebracht om de kwetsbaarheid te verhelpen. Zie bijgevoegde referenties voor meer informatie, waaronder achtergrondinformatie en IoC's.

Referenties

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-afw-zqYJkxjp>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-esa-dfCrfXkm>

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-76519	9.8 CRITICAL

CWE's

CWE	Beschrijving
CWE-23	Relative Path Traversal

Getroffen producten

Cisco
Cisco Secure Email

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.