Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0368

Kwetsbaarheid verholpen in Cisco Secure Email Gateway

NCSC Security Advisory

PRIORITEIT: HOOG

Gepubliceerd op: 14-09-2026

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 een kwetsbaarheid verholpen in Cisco Secure Email Gateway.

Duiding

De kwetsbaarheid bevindt zich in de verwerking van e-mailberichten binnen Cisco AsyncOS Software voor Cisco Secure Email Gateway en wordt veroorzaakt door onvoldoende validatie van inkomende e-mailberichten. Een niet-geauthenticeerde kwaadwillende kan een speciaal vervaardigd e-mailbericht met kwaadaardige SQL-instructies naar een kwetsbaar systeem versturen. Succesvol misbruik kan leiden tot het uitvoeren van willekeurige SQL-instructies en vervolgens tot het uitvoeren van willekeurige commando's met root-rechten op het onderliggende besturingssysteem.

Cisco meldt dat succesvolle exploitatie van deze kwetsbaarheid is waargenomen. Hoewel Cisco niet heeft vermeld op welke wijze de kwetsbaarheid wordt geëxploiteerd, raadt het NCSC dringend aan om de beveiligingsupdate zo snel mogelijk toe te passen en kwetsbare systemen te controleren op aanwijzingen van misbruik. Raadpleeg de advisory van Cisco voor IoC's en aanvullende informatie.

Oplossingen

Cisco heeft updates uitgebracht om de kwetsbaarheid te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-inj-2bLVGmhX

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-76461	9.8 CRITICAL

CWE's

CWE	Beschrijving
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

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 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.