Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2024-0311

Kwetsbaarheden verholpen in Cisco Secure Email Gateway

NCSC Advisory

PRIORITEIT: HOOG

Gepubliceerd op: 18-07-2024

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

Er zijn twee kwetsbaarheden verholpen in Cisco Secure Email Gateway.

Duiding

De meest ernstige kwetsbaarheid betreft CVE-2024-20401 en stelt een ongeauthenticeerde kwaadwillende in staat om middels het versturen van een mail met speciaal geprepareerde bijlage:

- Gebruikers met root rechten toe te voegen
- De configuratie van het apparaat aan te passen
- (Remote) code uit te voeren
- Een permanente Denial of Service (DoS) te veroorzaken.

CVE-2024-20429 betreft een Server-Side Template Injection en stelt een geauthenticeerde kwaadwillende met 'Operator' rechten in staat om op afstand code uit te voeren met root-rechten op het onderliggende OS.

Oplossingen

Cisco heeft updates beschikbaar gesteld om de kwetsbaarheden te verhelpen. Zie de referenties voor meer informatie.

Referenties

- https://nvd.nist.gov/vuln/detail/CVE-2024-20401
- https://nvd.nist.gov/vuln/detail/CVE-2024-20429
- https://www.cve.org/CVERecord?id=CVE-2024-20401
- https://www.cve.org/CVERecord?id=CVE-2024-20429
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-afw-bGG2UsjH
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-priv-esc-ssti-xNO2EOGZ

Kwetsbaarheden

CVE	CVSS Score
CVE-2024-20401	9.8 CRITICAL
CVE-2024-20429	6.5 MEDIUM

CWE's

CWE	Beschrijving
CWE-36	Absolute Path Traversal
CWE-74	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')
CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')

Getroffen producten

cisco
cisco_secure_email
secure_email

Disclaimer