Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0042

Kwetsbaarheden verholpen in Cisco AsyncOS Software

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 07-02-2025

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 kwetsbaarheden verholpen in Cisco AsyncOS Software (Specifiek voor Cisco Secure Web Appliance en Cisco Secure Email Gateway).

Duiding

De kwetsbaarheden bevinden zich in de manier waarop Cisco AsyncOS Software omgaat met verzoeken en configuratiebestanden. Een aanvaller kan ongeauthenticeerde toegang krijgen tot het systeem door gebruik te maken van onjuiste verwerking van opgemaakte range request headers, waardoor ze schadelijke bestanden kunnen downloaden zonder authenticatie. Daarnaast kunnen geauthenticeerde aanvallers, door onvoldoende validatie van XML-configuratiebestanden, commando-injectie aanvallen uitvoeren, wat kan leiden tot willekeurige commando-uitvoering. Bovendien kunnen lokale aanvallers een architectonale fout in het wachtwoordgeneratie-algoritme misbruiken, wat kan leiden tot privilege-escalatie naar root. Deze kwetsbaarheden vereisen onmiddellijke aandacht van beveiligingsteams.

Oplossingen

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

Referenties

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-sma-wsa-multi-yKUJhS34
- https://sec.cloudapps.cisco.com/security/center/publicationService.x?limit=20
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-swa-range-bypass-2BsEHYSu
- https://sec.cloudapps.cisco.com/security/center/publicationService.x?limit=20

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-20183	5.8 MEDIUM
CVE-2025-20184	6.5 MEDIUM
CVE-2025-20185	3.4 LOW

CWE's

CWE	Beschrijving
CWE-250	Execution with Unnecessary Privileges
CWE-20	Improper Input Validation

Getroffen producten

cisco
cisco_secure_email
cisco_secure_email_and_web_manager
cisco_secure_web_appliance

Disclaimer