Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0298

Kwetsbaarheden verholpen in Cisco Secure Firewall ASA en FTD

NCSC Advisory

PRIORITEIT: HOOG

Gepubliceerd op: 25-09-2025

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 Secure Firewall ASA en FTD Software.

Duiding

De kwetsbaarheid met kenmerk CVE-2025-20333, bevindt zich in de wijze waarop de software gebruikersinvoer in HTTP(S)-verzoeken valideert. Een aanvaller met geldige VPN-inloggegevens kan deze kwetsbaarheid misbruiken door speciaal vervaardigde HTTP-verzoeken naar een getroffen apparaat te sturen. Dit kan de aanvaller in staat stellen om willekeurige code uit te voeren met rootrechten, wat mogelijk leidt tot de volledige compromittering van het getroffen apparaat.

De kwetsbaarheid met kenmerk CVE-2025-20363, bevindt zich in de wijze waarop de software gebruikersinvoer in HTTP(S)-verzoeken valideert. Een aanvaller kan deze kwetsbaarheid misbruiken door speciaal vervaardigde HTTP-verzoeken te sturen naar een gerichte webservice op een getroffen apparaat, nadat hij aanvullende systeeminformatie heeft verkregen, exploit-mitigaties heeft omzeild, of beide. Een geslaagde exploit kan de aanvaller in staat stellen willekeurige code uit te voeren met rootrechten, wat kan leiden tot de volledige compromittering van het getroffen apparaat.

De kwetsbaarheid met kenmerk CVE-2025-20362, bevindt zich in de wijze waarop de software gebruikersinvoer in HTTP(S)-verzoeken valideert. Een aanvaller kan deze kwetsbaarheid misbruiken door speciaal vervaardigde HTTP-verzoeken naar een gerichte webserver op een apparaat te sturen. Een geslaagde exploit kan de aanvaller in staat stellen om zonder authenticatie toegang te krijgen tot een beperkt toegankelijke URL.

De kwetsbaarheden met kenmerk CVE-2025-20333 en CVE-2025-20363 zijn ernstig en vereisen onmiddellijke aandacht, aangezien ze kunnen leiden tot ongeautoriseerde controle over de systemen. Aanvallers kunnen deze kwetsbaarheden misbruiken om beveiligingsmaatregelen te omzeilen.

Cisco is op de hoogte van pogingen tot misbruik van deze kwetsbaarheid. Er is (nog) geen publieke Proof-of-Concept-code (PoC) of exploit beschikbaar.

Het NCSC verwacht dat PoC of Exploits binnen zeer korte termijn beschikbaar gaat komen, waarmee het risico op grootschalig misbruik toeneemt. Het NCSC adviseert met klem om deze updates zo snel mogelijk te installeren.

Oplossingen

Cisco heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Ook heeft Cisco Indicators of Compromise (IoC) gepubliceerd, waarmee kan worden onderzocht of een systeem is gecompromitteerd, en tijdelijke mitigatiestappen beschikbaar gesteld. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-webvpn-YROOTUW
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-webvpn-z5xP8EUB
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-http-code-exec-WmfP3h3O
- https://sec.cloudapps.cisco.com/security/center/resources/asa_ftd_continued_attacks
- https://sec.cloudapps.cisco.com/security/center/resources/detection_guide_for_continued_attacks

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-20333	9.9 CRITICAL
CVE-2025-20363	9.0 CRITICAL
CVE-2025-20362	6.5 MEDIUM

CWE's

CWE	Beschrijving
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
CWE-122	Heap-based Buffer Overflow
CWE-862	Missing Authorization

Getroffen producten

Cisco
ASA 5500
ASA 5500 Firmware
ASA 5500-X Series IPS SSP Software

Disclaimer