Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0264

Kwetsbaarheden verholpen in Cisco Secure Firewall Software

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 15-08-2025

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 meerdere kwetsbaarheden verholpen in Cisco Secure Firewall Software (inclusief ASA en FTD).

Duiding

De kwetsbaarheden bevinden zich in de manier waarop Cisco Secure Firewall de sleutel uitwisseling afhandeld (IKEv2), hiermee is het mogelijk voor een ongeauthenticeerde aanvaller om een Denial-of-Service aanval uit te voeren. De kwetsbaarheid met kenmerk CVE-2025-20265 bevind zich in de implementatie van het RADIUS-subsysteem, hierdoor is het mogelijk voor een ongeauthenticeerde kwaadwillende om willekeurige commando's uit te voeren op het onderliggende systeem.

Oplossingen

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

Referenties

- https://sec.cloudapps.cisco.com/security/center/viewErp.x?alertId=ERP-75415

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-20127	7.7 HIGH
CVE-2025-20133	8.6 HIGH
CVE-2025-20134	8.6 HIGH
CVE-2025-20135	4.3 MEDIUM
CVE-2025-20136	8.6 HIGH
CVE-2025-20148	8.5 HIGH
CVE-2025-20217	8.6 HIGH
CVE-2025-20218	4.9 MEDIUM

CVE-2025-20219	5.3 MEDIUM
CVE-2025-20220	6.0 MEDIUM
CVE-2025-20222	8.6 HIGH
CVE-2025-20224	5.8 MEDIUM
CVE-2025-20225	5.8 MEDIUM
CVE-2025-20235	6.1 MEDIUM
CVE-2025-20237	6.0 MEDIUM
CVE-2025-20238	6.0 MEDIUM
CVE-2025-20239	8.6 HIGH
CVE-2025-20243	8.6 HIGH
CVE-2025-20244	7.7 HIGH
CVE-2025-20251	8.5 HIGH
CVE-2025-20252	5.8 MEDIUM
CVE-2025-20253	8.6 HIGH
CVE-2025-20254	5.8 MEDIUM
CVE-2025-20263	8.6 HIGH
CVE-2025-20265	10.0 CRITICAL
CVE-2025-20268	5.8 MEDIUM
CVE-2025-20301	6.5 MEDIUM
CVE-2025-20302	4.3 MEDIUM
CVE-2025-20306	4.9 MEDIUM

CWE's

CWE	Beschrijving
CWE-146	Improper Neutralization of Expression/Command Delimiters
CWE-1244	Internal Asset Exposed to Unsafe Debug Access Level or State
CWE-643	Improper Neutralization of Data within XPath Expressions ('XPath Injection')
CWE-1287	Improper Validation of Specified Type of Input
CWE-229	Improper Handling of Values
CWE-415	Double Free
CWE-680	Integer Overflow to Buffer Overflow
CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')
CWE-404	Improper Resource Shutdown or Release
CWE-862	Missing Authorization
CWE-284	Improper Access Control
CWE-401	Missing Release of Memory after Effective Lifetime
CWE-74	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
CWE-835	Loop with Unreachable Exit Condition ('Infinite Loop')
CWE-20	Improper Input Validation
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Getroffen producten

Cisco
Cisco Firepower Management Center Appliances
Cisco Firepower Threat Defense Software
Cisco Secure Firewall 3100 Series
Cisco Secure Firewall 4200 Series
Cisco Adaptive Security Appliance (ASA) Software
Cisco Adaptive Security Virtual Appliance (ASAv)

Disclaimer