Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0077

Kwetsbaarheden verholpen in Cisco Secure Firewall systemen

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 05-03-2026

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

Duiding

De kwetsbaarheden omvatten SQL-injectie, privilege-escalatie, denial-of-service, cross-site scripting, en onjuist beheer van invoer in verschillende componenten van de Cisco Secure Firewall. Authenticated remote attackers kunnen deze kwetsbaarheden misbruiken om ongeautoriseerde toegang te krijgen, systeemintegriteit te compromitteren, of netwerkdiensten te verstoren. De kwetsbaarheden zijn aanwezig in de webinterfaces, REST API's, en andere functionaliteiten van de firewall software.

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-asa-dos-FCvLD6vR
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-scpcxt-filecpy-rgeP73nE
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ssh-keybypass-cr5xPUSf
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-aclbypass-dos-CVxVRSvQ
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-desync-n5AVzEQw
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-esp-dos-uv7yD8P5
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ikev2-dos-eBueGdEG
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-luainject-VescqgmS
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ospf-ZH8PhbSW
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-saml-LktTrwZP

› https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-vpn-dos-SpOFF2Re
› https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-vpn-m9sx6MbC
› https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-webvpn-xss-uwjc4HR
› https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-css-Fn4QSZ
› https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-cmd-inject-S9ZM4EJf
› https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-rce-NKhnULJh
› https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-sql-inject-2EnmTC8v
› https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-sql-injection-2qH6CcJd
› https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-cmd-inj-mTzGZexf
› https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-dnd-dos-bpEcg7B7
› https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-snort-bypass-rLggKzVF
› https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-snort3ssl-FBEKYXpH
› https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-tcp-dos-rHfqnwRg
› https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftdfmc-dir-trav-wERgjhWq
› https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-onprem-fmc-authbypass-5JPp45V2

Kwetsbaarheden

CVE	CVSS Score
› CVE-2024-20340	5.3 MEDIUM
› CVE-2024-20358	6.0 MEDIUM
› CVE-2026-20101	8.6 HIGH
› CVE-2026-20020	6.8 MEDIUM

CVE-2026-20073	5.8 MEDIUM
CVE-2026-20007	5.8 MEDIUM
CVE-2026-20018	5.9 MEDIUM
CVE-2026-20002	8.1 HIGH
CVE-2026-20015	5.8 MEDIUM
CVE-2026-20062	7.2 HIGH
CVE-2026-20031	5.3 MEDIUM
CVE-2026-20039	8.6 HIGH
CVE-2026-20022	6.1 MEDIUM
CVE-2026-20050	6.8 MEDIUM
CVE-2026-20069	4.3 MEDIUM
CVE-2026-20009	5.3 MEDIUM
CVE-2026-20014	7.7 HIGH
CVE-2026-20016	6.0 MEDIUM
CVE-2026-20021	4.3 MEDIUM
CVE-2026-20049	7.7 HIGH
CVE-2026-20105	7.7 HIGH
CVE-2026-20025	6.8 MEDIUM
CVE-2026-20082	8.6 HIGH
CVE-2026-20006	5.8 MEDIUM
CVE-2026-20103	8.6 HIGH
CVE-2026-20008	6.0 MEDIUM
CVE-2026-20063	6.0 MEDIUM

CVE-2026-20106	5.3 MEDIUM
CVE-2026-20017	6.0 MEDIUM
CVE-2026-20100	7.7 HIGH
CVE-2026-20044	6.0 MEDIUM
CVE-2026-20024	6.8 MEDIUM
CVE-2026-20064	6.5 MEDIUM
CVE-2026-20023	6.1 MEDIUM
CVE-2026-20003	4.9 MEDIUM
CVE-2026-20102	6.1 MEDIUM
CVE-2026-20013	5.8 MEDIUM
CVE-2026-20070	6.1 MEDIUM
CVE-2026-20001	6.5 MEDIUM
CVE-2026-20052	5.8 MEDIUM

CWE's

CWE	Beschrijving
CWE-20	Improper Input Validation
CWE-27	Path Traversal: 'dir/../../filename'
CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-80	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)

CWE-88	Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
CWE-131	Incorrect Calculation of Buffer Size
CWE-138	Improper Neutralization of Special Elements
CWE-190	Integer Overflow or Wraparound
CWE-244	Improper Clearing of Heap Memory Before Release ('Heap Inspection')
CWE-248	Uncaught Exception
CWE-250	Execution with Unnecessary Privileges
CWE-269	Improper Privilege Management
CWE-279	Incorrect Execution-Assigned Permissions
CWE-284	Improper Access Control
CWE-330	Use of Insufficiently Random Values
CWE-388	CWE-388
CWE-401	Missing Release of Memory after Effective Lifetime
CWE-404	Improper Resource Shutdown or Release
CWE-444	Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')
CWE-476	NULL Pointer Dereference
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-772	Missing Release of Resource after Effective Lifetime
CWE-787	Out-of-bounds Write
CWE-788	Access of Memory Location After End of Buffer
CWE-823	Use of Out-of-range Pointer Offset

Getroffen producten

Cisco
Adaptive Security Appliance
Cisco 3000 Series Industrial Security Appliances (ISA)
Cisco ASA 5500-X Series Firewalls
Cisco Adaptive Security Virtual Appliance (ASAv)
Cisco Firepower 1000 Series
Cisco Firepower 2100 Series
Cisco Firepower 9000 Series
Cisco Secure Endpoint
Cisco Secure Firewall 3100 Series
Cisco Secure Firewall 4200 Series
Cisco Secure Firewall Adaptive Security Appliance (ASA) Software
Cisco Secure Firewall Management Center
Cisco Secure Firewall Management Center (FMC)
Cisco Secure Firewall Management Center (FMC) Appliances

Cisco Secure Firewall Threat Defense (FTD) Software
Firepower Management Center
Firepower Threat Defense

Disclaimer