

CVE-2025-20362

Cisco Secure Firewall Adaptive Security (ASA) Appliance and Secure Firewall Threat Defense (FTD) Missing Authorization Vulnerability

CISA KEV since Sep 25, 2025

Actively exploited

Update: On November 5, 2025, Cisco became aware of a new attack variant against devices running Cisco Secure ASA Software or Cisco Secure FTD Software releases that are affected by CVE-2025-20333 and CVE-2025-20362. This attack can cause unpatched devices to unexpectedly reload, leading to denial of service (DoS) conditions. Cisco strongly recommends that all customers upgrade to the fixed software releases that are listed in the Fixed Software ["#fs"] section of this advisory.

EVRS 83 / ₁₀₀ Urgent priority	CVSS V3.1 8.6 High · NVD	EPSS 0.871 99.75th percentile · FIRST	CISA DEADLINE Sep 26, 2025 KEV since 2025 · listed over a year
---	--	---	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	Added to CISA KEV within the last two years
☒ EPSS	0.871 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.6	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: The KEV due date refers to the deadline by which FCEB agencies are expected to review and begin implementing the guidance outlined in Emergency Directive (ED) 25-03 (URL listed below in Notes). Agencies must follow the mitigation steps provided by CISA (URL listed below in Notes) and vendor's instructions (URL listed below in Notes). Adhere to the applicable BOD 22-01 guidance for cloud services or discontinue use of the product if mitigations are not available.

Basis: CISA KEV required action

A vulnerability in the VPN web server of Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to access restricted URL endpoints that are related to remote access VPN that should otherwise be inaccessible without authentication. This vulnerability is due to improper validation of user-supplied input in HTTP(S) requests. An attacker could exploit this vulnerability by sending crafted HTTP requests to a targeted web server on a device. A successful exploit could allow the attacker to access a restricted URL without authentication.

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
secure firewall threat defense	$\geq 7.0.0 < 7.0.8.1$ $\geq 7.1.0 < 7.2.10.2$ $\geq 7.3.0 < 7.4.2.4$ $\geq 7.6.0 < 7.6.2.1$ $\geq 7.7.0 < 7.7.10.1$	no fixed version listed	NVD
adaptive security appliance software	$\geq 9.12 < 9.12.4.72$ $\geq 9.14 < 9.14.4.28$ $\geq 9.16 < 9.16.4.85$ $\geq 9.17.0 < 9.18.4.67$ $\geq 9.19 < 9.20.4.10$ $\geq 9.22 < 9.22.2.14$ $\geq 9.23 < 9.23.1.19$	9.12.4.72 · 9.14.4.28 · 9.16.4.85 · 9.18.4.67 · 9.20.4.10 · 9.22.2.14	NVD

Sources

Vendor guidance	sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asafth-webvpn-YR00TUW	CISA Mitigation Instructions	cisa.gov/news-events/directives/ed-25-03-identify-and-mitigate-potential-compromise-cisco-devices
cisa.gov	cisa.gov/news-events/directives/supplemental-direction-ed-25-03-core-dump-and-hunt-instructions	cisa.gov	cisa.gov/eviction-strategies-tool/create-from-template
sec.cloudapps.cisco.com	sec.cloudapps.cisco.com/security/center/resources/asa_ftd_continued_attacks	sec.cloudapps.cisco.com	sec.cloudapps.cisco.com/security/center/private/resources/asa_ftd_continued_attacks#Details
NVD	nvd.nist.gov/vuln/detail/CVE-2025-20362	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2025-31139	Current data	evulnable.com/vulnerability-management/cve/CVE-2025-20362

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.