

CVE-2026-20349

Cisco Secure Firewall Adaptive Security Appliance (ASA) and Secure Firewall Threat Defense (FTD) Heap Inspection Vulnerability

CISA KEV since Aug 11, 2026

Actively exploited

A vulnerability in the Remote Access SSL VPN service for Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient error checking when processing HTTP requests.

EVRS 75 / ₁₀₀ Urgent priority	CVSS V3.1 8.6 High · NVD	EPSS 0.010 62.8th percentile · FIRST	CISA DEADLINE Aug 14, 2026 CISA federal deadline · Overdue by 2 months
---	--	--	--

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 90 days
☒ EPSS	0.010 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: Apply mitigations in accordance with vendor instructions, ensuring compliance with CISA's BOD 26-04 Prioritizing Security Updates Based on Risk (see URL in Notes) guidance and CISA's "Forensics Triage Requirements" (see URL in Notes). Follow applicable BOD 26-04 guidance for cloud services or discontinue use of the product if mitigations are unavailable. Stakeholders are responsible for evaluating each asset's internet exposure and ensuring adherence to BOD 26-04 patching guidelines.

Basis: CISA KEV required action

An attacker could exploit this vulnerability by sending a crafted HTTP request to the Remote Access SSL VPN service on an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition.

Affected and fixed versions



secure firewall threat defense	7.0.0	no fixed version listed	NVD
	7.0.0.1		
	7.0.1		
	7.0.1.1		
	7.0.2		
	7.0.2.1		
	7.0.3		
	7.0.4		
	7.0.5		
	7.0.6		
	7.0.6.1		
	7.0.6.2		
	7.0.6.3		
	7.0.7		
	7.0.8		
	7.0.8.1		
	7.0.9		
	7.2.0		
	7.2.0.1		
	7.2.1		
	7.2.2		
	7.2.3		
	7.2.4		
	7.2.4.1		
	7.2.5		
	7.2.5.1		
	7.2.5.2		
	7.2.6		
	7.2.7		
	7.2.8		
	7.2.8.1		
	7.2.9		
	7.2.10		
	7.2.10.2		
	7.2.11		
	7.2.12		
	7.3.0		
	7.3.1		
	7.3.1.1		
	7.3.1.2		
	7.4.0		
	7.4.1		
	7.4.1.1		
	7.4.2		
	7.4.2.1		
	7.4.2.2		
	7.4.2.3		
	7.4.2.4		
	7.4.3		
	7.4.4		
	7.4.7		
	7.4.8		
	7.6.0		
	7.6.1		
	7.6.2		
	7.6.2.1		
	7.6.4		
	7.7.0		
	7.7.10		
	7.7.10.1		
	7.7.11		
	7.7.13		
	10.0.0		



10.0.2

adaptive security appliance	9.16.1	no fixed version listed	NVD
software	9.16.1.28		
	9.16.2		
	9.16.2.3		
	9.16.2.7		
	9.16.2.11		
	9.16.2.13		
	9.16.2.14		
	9.16.3		
	9.16.3.3		
	9.16.3.14		
	9.16.3.15		
	9.16.3.19		
	9.16.3.23		
	9.16.4		
	9.16.4.9		
	9.16.4.14		
	9.16.4.19		
	9.16.4.27		
	9.16.4.38		
	9.16.4.39		
	9.16.4.42		
	9.16.4.48		
	9.16.4.55		
	9.16.4.57		
	9.16.4.61		
	9.16.4.62		
	9.16.4.67		
	9.16.4.70		
	9.16.4.71		
	9.16.4.76		
	9.16.4.82		
	9.16.4.84		
	9.16.4.85		
	9.16.4.89		
	9.16.4.92		
	9.18.1		
	9.18.1.3		
	9.18.2		
	9.18.2.5		
	9.18.2.7		
	9.18.2.8		
	9.18.3		
	9.18.3.39		
	9.18.3.46		
	9.18.3.53		
	9.18.3.55		
	9.18.3.56		
	9.18.4		
	9.18.4.5		
	9.18.4.8		
	9.18.4.22		
	9.18.4.24		
	9.18.4.29		
	9.18.4.34		
	9.18.4.40		
	9.18.4.47		
	9.18.4.50		
	9.18.4.52		
	9.18.4.53		
	9.18.4.57		
	9.18.4.66		
	9.18.4.67		

9.18.4.68
9.18.4.71
9.18.4.76
9.18.4.82
9.18.4.90
9.18.4.135
9.19.1
9.19.1.5
9.19.1.9
9.19.1.12
9.19.1.18
9.19.1.22
9.19.1.24
9.19.1.27
9.19.1.28
9.19.1.31
9.19.1.37
9.19.1.38
9.19.1.42
9.20.1
9.20.1.5
9.20.2
9.20.2.10
9.20.2.21
9.20.2.22
9.20.3
9.20.3.4
9.20.3.7
9.20.3.9
9.20.3.10
9.20.3.13
9.20.3.16
9.20.3.20
9.20.4
9.20.4.7
9.20.4.10
9.20.4.14
9.20.4.19
9.20.4.22
9.20.4.28
9.20.4.30
9.20.4.34
9.20.4.46
9.22.1.1
9.22.1.2
9.22.1.3
9.22.1.6
9.22.2
9.22.2.4
9.22.2.9
9.22.2.13
9.22.2.14
9.22.2.20
9.22.2.32
9.22.3
9.22.3.5
9.23.1
9.23.1.3
9.23.1.7
9.23.1.13
9.23.1.19
9.23.1.22
9.23.1.26
9.23.1.32



PACKAGE	AFFECTED	FIXED IN	SOURCE
	9.23.1.195		
	9.24.1		
	9.24.1.5		
	9.24.1.9		
	9.24.1.11		
	9.24.1.155		

Sources

Vendor guidance	github.com/advisories/GHSA-8x4j-5v9x-9frv	sec.cloudapps.cisco.com	sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-vpn-dos-dzv4mQFF
BOD 26-04	cisa.gov/news-events/directives/bod-26-04-prioritizing-security-updates-based-risk	Forensics Triage Requirements	cisa.gov/news-events/directives/bod-26-04-implementation-guidance-prioritizing-security-updates-based-risk
NVD	nvd.nist.gov/vuln/detail/CVE-2026-20349	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-56643	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-20349

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