

CVE-2020-3259

Cisco ASA and FTD Information Disclosure Vulnerability

CISA KEV since Feb 15, 2024

Actively exploited

Ransomware use known

A vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to retrieve memory contents on an affected device, which could lead to the disclosure of confidential information. The vulnerability is due to a buffer tracking issue when the software parses invalid URLs that are requested from the web services interface.

EVRS 83/100 Urgent priority	CVSS V3.1 7.5 High · NVD	EPSS 0.715 99.42nd percentile · FIRST	CISA DEADLINE Mar 7, 2024 KEV since 2024 · 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	Known ransomware campaigns	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.715 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.5	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
Basis: CISA KEV required action

An attacker could exploit this vulnerability by sending a crafted GET request to the web services interface. A successful exploit could allow the attacker to retrieve memory contents, which could lead to the disclosure of confidential information. Note: This vulnerability affects only specific AnyConnect and WebVPN configurations. For more information, see the Vulnerable Products section.

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
secure firewall threat defense	$\geq 6.2.3 < 6.2.3.16$ $\geq 6.3.0 < 6.3.0.6$ $\geq 6.4.0 < 6.4.0.9$ $\geq 6.5.0 < 6.5.0.5$	6.2.3.16 · 6.3.0.6 · 6.4.0.9 · 6.5.0.5	NVD
adaptive security appliance software	$\geq 9.8 < 9.8.4.20$ $\geq 9.9 < 9.9.2.67$ $\geq 9.10 < 9.10.1.40$ $\geq 9.12 < 9.12.3.9$ $\geq 9.13 < 9.13.1.10$	9.8.4.20 · 9.9.2.67	NVD

Sources

Vendor guidance	tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asafthd-info-disclose-9eJtycMB	NVD	nvd.nist.gov/vuln/detail/CVE-2020-3259
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2020-24530
Current data	evulnable.com/vulnerability-management/cve/CVE-2020-3259		

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