

CVE-2023-20269

Cisco Adaptive Security Appliance and Firepower Threat Defense Unauthorized Access Vulnerability

Exigent

CISA KEV since Sep 13, 2023

Actively exploited

Ransomware use known

A vulnerability in the remote access VPN feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct a brute force attack in an attempt to identify valid username and password combinations or an authenticated, remote attacker to establish a clientless SSL VPN session with an unauthorized user.

EVRS 85/100 Immediate priority	CVSS V3.1 9.1 Critical · NVD	EPSS 0.255 97.9th percentile · FIRST	CISA DEADLINE Oct 4, 2023 KEV since 2023 · 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	0.255 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.1	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions for group-lock and vpn-simultaneous-logins or discontinue use of the product for unsupported devices.

Basis: CISA KEV required action

This vulnerability is due to improper separation of authentication, authorization, and accounting (AAA) between the remote access VPN feature and the HTTPS management and site-to-site VPN features. An attacker could exploit this vulnerability by specifying a default connection profile/tunnel group while conducting a brute force attack or while establishing a clientless SSL VPN session using valid credentials. A successful exploit could allow the attacker to achieve one or both of the following: Identify valid credentials that could then be used to establish an unauthorized remote access VPN session. Establish a clientless SSL VPN session (only when running Cisco ASA Software Release 9.16 or earlier). Notes: Establishing a client-based remote access VPN tunnel is not possible as these default connection profiles/tunnel groups do not and cannot have an IP address pool configured. This vulnerability does not allow an attacker to bypass authentication. To successfully establish a remote access VPN session, valid credentials are required, including a valid second factor if multi-factor authentication (MFA) is configured. Cisco will release software updates that address this vulnerability. There are workarounds that address this vulnerability.

Affected and fixed versions



secure firewall threat defense	6.2.3	no fixed version listed	NVD
	6.2.3.1		
	6.2.3.2		
	6.2.3.3		
	6.2.3.4		
	6.2.3.5		
	6.2.3.6		
	6.2.3.7		
	6.2.3.8		
	6.2.3.9		
	6.2.3.10		
	6.2.3.11		
	6.2.3.12		
	6.2.3.13		
	6.2.3.14		
	6.2.3.15		
	6.2.3.16		
	6.2.3.17		
	6.2.3.18		
	6.4.0		
	6.4.0.1		
	6.4.0.2		
	6.4.0.3		
	6.4.0.4		
	6.4.0.5		
	6.4.0.6		
	6.4.0.7		
	6.4.0.8		
	6.4.0.9		
	6.4.0.10		
	6.4.0.11		
	6.4.0.12		
	6.4.0.13		
	6.4.0.14		
	6.4.0.15		
	6.4.0.16		
	6.6.0		
	6.6.0.1		
	6.6.1		
	6.6.3		
	6.6.4		
	6.6.5		
	6.6.5.1		
	6.6.5.2		
	6.6.7		
	6.6.7.1		
	6.7.0		
	6.7.0.1		
	6.7.0.2		
	6.7.0.3		
	7.0.0		
	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		
	7.1.0		
	7.1.0.1		
	7.1.0.2		



7.1.0.3
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
7.3.0
7.3.1
7.3.1.1
7.4.0



adaptive security appliance	9.8.1	no fixed version listed	NVD
software	9.8.1.5		
	9.8.1.7		
	9.8.2		
	9.8.2.8		
	9.8.2.14		
	9.8.2.15		
	9.8.2.17		
	9.8.2.20		
	9.8.2.24		
	9.8.2.26		
	9.8.2.28		
	9.8.2.33		
	9.8.2.35		
	9.8.2.38		
	9.8.3		
	9.8.3.8		
	9.8.3.11		
	9.8.3.14		
	9.8.3.16		
	9.8.3.18		
	9.8.3.21		
	9.8.3.26		
	9.8.3.29		
	9.8.4		
	9.8.4.3		
	9.8.4.7		
	9.8.4.8		
	9.8.4.10		
	9.8.4.12		
	9.8.4.15		
	9.8.4.17		
	9.8.4.20		
	9.8.4.22		
	9.8.4.25		
	9.8.4.26		
	9.8.4.29		
	9.8.4.32		
	9.8.4.33		
	9.8.4.34		
	9.8.4.35		
	9.8.4.39		
	9.8.4.40		
	9.8.4.41		
	9.8.4.43		
	9.8.4.44		
	9.8.4.45		
	9.8.4.46		
	9.8.4.48		
	9.12.1		
	9.12.1.2		
	9.12.1.3		
	9.12.2		
	9.12.2.1		
	9.12.2.4		
	9.12.2.5		
	9.12.2.9		
	9.12.3		
	9.12.3.2		
	9.12.3.7		
	9.12.3.9		
	9.12.3.12		
	9.12.4		

9.12.4.2
9.12.4.4
9.12.4.7
9.12.4.8
9.12.4.10
9.12.4.13
9.12.4.18
9.12.4.24
9.12.4.26
9.12.4.29
9.12.4.30
9.12.4.35
9.12.4.37
9.12.4.38
9.12.4.39
9.12.4.40
9.12.4.41
9.12.4.47
9.12.4.48
9.12.4.50
9.12.4.52
9.12.4.54
9.12.4.55
9.12.4.56
9.12.4.58
9.14.1
9.14.1.6
9.14.1.10
9.14.1.15
9.14.1.19
9.14.1.30
9.14.2
9.14.2.4
9.14.2.8
9.14.2.13
9.14.2.15
9.14.3
9.14.3.1
9.14.3.9
9.14.3.11
9.14.3.13
9.14.3.15
9.14.3.18
9.14.4
9.14.4.6
9.14.4.7
9.14.4.12
9.14.4.13
9.14.4.14
9.14.4.15
9.14.4.17
9.14.4.22
9.14.4.23
9.15.1
9.15.1.1
9.15.1.7
9.15.1.10
9.15.1.15
9.15.1.16
9.15.1.17
9.15.1.21
9.16.1
9.16.1.28
9.16.2



PACKAGE	AFFECTED	FIXED IN	SOURCE
	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		
	9.16.4.18		
	9.16.4.19		
	9.16.4.27		
	9.16.4.38		
	9.17.1		
	9.17.1.7		
	9.17.1.9		
	9.17.1.10		
	9.17.1.11		
	9.17.1.13		
	9.17.1.15		
	9.17.1.20		
	9.17.1.30		
	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		
	9.19.1		
	9.19.1.5		
	9.19.1.9		
	9.19.1.12		
	9.19.1.18		

Sources

Vendor guidance github.com/advisories/GHSA-v7pw-9cmm-88m6

Additional guidance sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ravpn-auth-8LyfCkeC
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog
Current data evulnable.com/vulnerability-management/cve/CVE-2023-20269

NVD nvd.nist.gov/vuln/detail/CVE-2023-20269

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2023-24448

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