

CVE-2016-6367

Cisco Adaptive Security Appliance (ASA) CLI Remote Code Execution Vulnerability

CISA KEV since May 24, 2022

Actively exploited

Cisco Adaptive Security Appliance (ASA) Software before 8.4(1) on ASA 5500, ASA 5500-X, PIX, and FWSM devices allows local users to gain privileges via invalid CLI commands, aka Bug ID CSCtu74257 or EPICBANANA.

EVRS 75 _{/100} Urgent priority	CVSS V3.1 7.8 High · NVD	EPSS 0.226 97.7th percentile · FIRST	CISA DEADLINE Jun 14, 2022 KEV since 2022 · 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	On the CISA KEV catalog for over two years
☒ EPSS	0.226 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified**CISA required action:** Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions · 22 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
adaptive security appliance software	≥ 7.2.0 < 8.4\ (3\) ≥ 8.5 < 9.0\ (1\)	8.4\ (3\) · 9.0\ (1\)	NVD
asa 5500	—	no fixed version listed	NVD
asa 5500-x	—	no fixed version listed	NVD
asa 5500 csc-ssm	—	no fixed version listed	NVD
asa 5505	—	no fixed version listed	NVD
asa 5506-x	—	no fixed version listed	NVD
asa 5506h-x	—	no fixed version listed	NVD
asa 5506w-x	—	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-cxx8-9qq9-rm4x	NVD	nvd.nist.gov/vuln/detail/CVE-2016-6367
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2016-7290
Current data	evulnable.com/vulnerability-management/cve/CVE-2016-6367		

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