

CVE-2016-6366

Cisco Adaptive Security Appliance (ASA) SNMP Buffer Overflow Vulnerability

CISA KEV since May 24, 2022

Actively exploited

Public exploit module (Metasploit)

Buffer overflow in Cisco Adaptive Security Appliance (ASA) Software through 9.4.2.3 on ASA 5500, ASA 5500-X, ASA Services Module, ASA 1000V, ASAv, Firepower 9300 ASA Security Module, PIX, and FWSM devices allows remote authenticated users to execute arbitrary code via crafted IPv4 SNMP packets, aka Bug ID CSCva92151 or EXTRABACON.

EVRS 82/₁₀₀ Urgent priority	CVSS V3.1 8.8 High · NVD	EPSS 0.876 99.76th 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	0.876 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.8	☐ 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 · 37 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
pix firewall software	–	no fixed version listed	NVD
adaptive security appliance software	$\geq 7.2.1 < 9.0.4.40$ $\geq 9.1.1 < 9.1.7(9)$ $\geq 9.2.0 < 9.2.4(14)$ $\geq 9.3.0 < 9.3.3(10)$ $\geq 9.4.0.115 < 9.4.3(8)$ $\geq 9.5.0 \leq 9.5(3)$ $\geq 9.6.0 < 9.6.1(11)$	$9.0.4.40 \cdot 9.1.7(9) \cdot$ $9.2.4(14) \cdot 9.3.3(10) \cdot$ $9.4.3(8) \cdot \text{after } 9.5(3)$	NVD
asa 1000v cloud firewall software	8.7.1 8.7.1.1	no fixed version listed	NVD
pix firewall 501	–	no fixed version listed	NVD
pix firewall 506	–	no fixed version listed	NVD
pix firewall 506e	–	no fixed version listed	NVD
pix firewall 515	–	no fixed version listed	NVD
pix firewall 515e	–	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-pfgh-2mw6-962h	NVD	nvd.nist.gov/vuln/detail/CVE-2016-6366
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2016-7289
Current data	evulnable.com/vulnerability-management/cve/CVE-2016-6366		

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