

CVE-2017-15944

Palo Alto Networks PAN-OS Remote Code Execution Vulnerability

Exigent

CISA KEV since Aug 18, 2022

Actively exploited

Public exploit module (Metasploit)

Palo Alto Networks PAN-OS before 6.1.19, 7.0.x before 7.0.19, 7.1.x before 7.1.14, and 8.0.x before 8.0.6 allows remote attackers to execute arbitrary code via vectors involving the management interface.

EVRS 87 / 100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.983 99.92nd percentile · FIRST	CISA DEADLINE Sep 8, 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	0.983 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

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

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
pan-os	< 6.1.19 ≥ 7.0.0 < 7.0.19 ≥ 7.1.0 < 7.1.14 ≥ 8.0.0 < 8.0.6	6.1.19 · 7.0.19 · 7.1.14 · 8.0.6	NVD

Sources

Vendor guidance github.com/advisories/GHSA-9ppr-hv62-39w2
NVD nvd.nist.gov/vuln/detail/CVE-2017-15944

Additional guidance security.paloaltonetworks.com/CVE-2017-15944
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2017-7360

Current data evulnable.com/vulnerability-management/cve/CVE-2017-15944

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