

CVE-2024-9474

Palo Alto Networks PAN-OS Management Interface OS Command Injection Vulnerability

CISA KEV since Nov 18, 2024

Actively exploited

Ransomware use known

Public exploit module (Metasploit)

A privilege escalation vulnerability in Palo Alto Networks PAN-OS software allows a PAN-OS administrator with access to the management web interface to perform actions on the firewall with root privileges. Cloud NGFW and Prisma Access are not impacted by this vulnerability.

EVRS

89/100

Immediate priority

CVSS V4.0

6.9

Medium · NVD

EPSS

0.948

99.86th percentile · FIRST

CISA DEADLINE

Dec 9, 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	Added to CISA KEV within the last two years
☒ EPSS	0.948 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 6.9	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch Immediately Patch or fixed version identified**CISA required action:** Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

Additionally, the management interfaces for affected devices should not be exposed to untrusted networks, including the internet.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
pan-os	≥ 10.1.0 < 10.1.14 ≥ 10.2.0 < 10.2.12 ≥ 11.0.0 < 11.0.6 ≥ 11.1.0 < 11.1.5 ≥ 11.2.0 < 11.2.4 10.1.14 10.2.12 11.0.6 11.1.5 11.2.4	10.1.14 · 10.2.12 · 11.0.6 · 11.1.5 · 11.2.4	NVD

Sources

Vendor guidance	security.paloaltonetworks.com/CVE-2024-9474	NVD	nvd.nist.gov/vuln/detail/CVE-2024-9474
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2024-50354
Current data	evulnable.com/vulnerability-management/cve/CVE-2024-9474		

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