

CVE-2024-9463

Palo Alto Networks Expedition OS Command Injection Vulnerability

Exigent

CISA KEV since Nov 14, 2024

Actively exploited

An OS command injection vulnerability in Palo Alto Networks Expedition allows an unauthenticated attacker to run arbitrary OS commands as root in Expedition, resulting in disclosure of usernames, cleartext passwords, device configurations, and device API keys of PAN-OS firewalls.

EVRS 88/100 Immediate priority	CVSS V4.0 9.9 Critical · NVD	EPSS 0.985 99.92nd percentile · FIRST	CISA DEADLINE Dec 5, 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	No known ransomware campaign association	☐ KEV recency	Added to CISA KEV within the last two years
☒ EPSS	0.985 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.9	☐ 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 or discontinue use of the product if mitigations are unavailable.
Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
expedition	≥ 1.2.0 < 1.2.96	1.2.96	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-r2fh-mj7f-v33r	Additional guidance	security.paloaltonetworks.com/PAN-SA-2024-0010
NVD	nvd.nist.gov/vuln/detail/CVE-2024-9463	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2024-49955	Current data	evulnable.com/vulnerability-management/cve/CVE-2024-9463

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