

CVE-2024-5910

Palo Alto Networks Expedition Missing Authentication Vulnerability

Exigent

CISA KEV since Nov 7, 2024

Actively exploited

Public exploit module (Metasploit)

Missing authentication for a critical function in Palo Alto Networks Expedition can lead to an Expedition admin account takeover for attackers with network access to Expedition. Note: Expedition is a tool aiding in configuration migration, tuning, and enrichment. Configuration secrets, credentials, and other data imported into Expedition is at risk due to this issue.

EVRS 85/100 Immediate priority	CVSS V4.0 9.3 Critical · NVD	EPSS 0.917 99.82nd percentile · FIRST	CISA DEADLINE Nov 28, 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	0.917 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.3	☐ 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 < 1.2.92	1.2.92	NVD

Sources

Vendor guidance github.com/advisories/GHSA-px3f-fc5j-2fqv
NVD nvd.nist.gov/vuln/detail/CVE-2024-5910

Additional guidance security.paloaltonetworks.com/CVE-2024-5910
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2024-47042

Current data evulnable.com/vulnerability-management/cve/CVE-2024-5910

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