*CYBER ADVISORY*

TLP:CLEAR
09 OCT 2024

# Palo Alto Expedition Multiple Firewall Takeover Vulnerabilities

Palo Alto | Firewall | Expedition | Critical

---

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of multiple critical vulnerabilities affecting Palo Alto Networks Expedition solution, with proof on concept available.[1] Exploitation of these vulnerabilities may allow an unauthenticated attacker to take over firewall admin accounts, exposing sensitive information, including usernames, cleartext passwords, and API keys for PAN-OS firewalls. [2]

The Cal-CSIC recommends immediately updating Expedition to version 1.2.96.

For further information on updating Palo Alto Expedition and mitigations, please refer to PAN-SA-2024-0010 Expedition: Multiple Vulnerabilities Lead to Firewall Admin Account Takeover (paloaltonetworks.com) [3]

| Issue | CVE Identifier(s) | CVSS v4.0 |
|---|---|---|
| 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 | **CVE-2024-9463** | **9.9** |
| An OS command injection vulnerability in Palo Alto Networks Expedition allows an authenticated 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 | **CVE-2024-9464** | **9.3** |
| An SQL injection vulnerability in Palo Alto Networks Expedition allows an unauthenticated attacker to reveal Expedition database contents, such as password hashes, usernames, device configurations, and device API keys. With this, attackers can also create and read arbitrary files on the Expedition system | **CVE-2024-9465** | **9.2** |
| A cleartext storage of sensitive information vulnerability in Palo Alto Networks Expedition allows an authenticated attacker to reveal firewall usernames, passwords, and API keys generated using those credentials | **CVE-2024-9466** | **8.2** |

| | | |
|---|---|---|
| A reflected XSS vulnerability in Palo Alto Networks Expedition enables execution of malicious JavaScript in the context of an authenticated Expedition user's browser if that user clicks on a malicious link, allowing phishing attacks that could lead to Expedition browser session theft | **CVE-2024-9467** | **7.0** |

**Table 1: Multiple Palo Alto Networks Expedition Critical Vulnerabilities** [3]

## Organization, Source, Reference, and Dissemination Information

| | |
|---|---|
| **Organization Description** | California Government Code § 8586.5 established the California Cybersecurity Integration Center (Cal-CSIC) as the central organizing hub of state government's cybersecurity activities, including information sharing, intelligence analysis, incident response, and overarching cybersecurity strategy. The Cal-CSIC is responsible for reducing the likelihood and severity of cyber incidents that could damage California's economy, critical infrastructure, and public or private sector networks in our state. |
| **Customer Feedback** | If you need further information about this issue, contact the Cal-CSIC at our email address CalCSIC@caloes.ca.gov or by telephone at (833) REPORT1. To help us identify ways to better assist you, please submit feedback calcsic@caloes.ca.gov. |
| **Source Summary Statement** | This report was compiled from a variety of sources, predominately open-source reporting. |
| **Handling Caveats** | **Traffic Light Protocol (TLP):** Recipients may share TLP:CLEAR information with the world; there is no limit on disclosure. Subject to standard copyright TLP:CLEAR rules, information may be shared without restriction. |
| **Information Needs** | *HSEC 1.1; HSEC 1.2; HSEC 1.5; HSEC 1.8; HSEC 1.10; STAC KIQ 1.1; KIQ 1.2; KIQ 1.3; KIQ 1.4; KIQ 1.5* |

[1] Bleeping Computer; "Palo Alto Networks Warn of Firewall Hijack Bug With Public Exploit" https://www.bleepingcomputer.com/news/security/palo-alto-networks-warns-of-firewall-hijack-bugs-with-public-exploit/; accessed 09 October 2024

[2] Cybersecurity News; "Palo Alto Networks Issues Fix for Critical Vulnerabilities; Including CVE-2024-9463 (CVSS 9.9)" https://securityonline.info/palo-alto-networks-issues-fix-for-critical-vulnerabilities-including-cve-2024-9463-cvss-9-9/;accessed 09 October 2024

[3] Palo Alto Networks; "PANS-SA-2024-0010 Expedition: Multiple Vulnerabilities Lead to Firewall Admin Account Takeover" https://security.paloaltonetworks.com/PAN-SA-2024-0010; accessed 09 October 2024