CERT-EU

### Security Advisory 2024-108

# Palo Alto Critical Vulnerabilities

*2024-10-11 — v1.0*

**TLP:CLEAR**

*History:*

- *11/10/2024 — v1.0 – Initial publication*

## Summary

Palo Alto Networks has disclosed multiple critical vulnerabilities in its Expedition tool that can lead to unauthorised access to firewall credentials and sensitive data, including usernames, passwords, and API keys. The vulnerabilities allow attackers to execute arbitrary commands, read or write files, and exploit SQL injection flaws. Successful exploitation could result in a full takeover of affected systems.

## Technical Details

The vulnerabilities include:

- **CVE-2024-9463**: OS command injection allowing unauthenticated attackers to execute commands as root (CVSS 9.9).
- **CVE-2024-9464**: Authenticated OS command injection (CVSS 9.3).
- **CVE-2024-9465**: SQL injection leading to credential exposure and file access (CVSS 9.2).
- **CVE-2024-9466**: Clear-text storage of sensitive information (CVSS 8.2).
- **CVE-2024-9467**: Reflected XSS vulnerability enabling JavaScript execution (CVSS 7.0).

## Affected Products

- Expedition versions prior to 1.2.96.

## Detection

In the `/var/apache/log/access.log` file, anomalous calls to the following endpoints might indicate abuse of these vulnerabilities:

- `/OS/startup/restore/restoreAdmin.php`
- `/bin/CronJobs.php`
- `/bin/configurations/parsers/Checkpoint/CHECKPOINT.php`

## Recommendations

It is recommended to upgrade to Expedition 1.2.96 or later to mitigate these vulnerabilities. The access and exposure to Expedition should also be limited.

## References

[1] https://security.paloaltonetworks.com/PAN-SA-2024-0010

[2] https://www.securityweek.com/palo-alto-patches-critical-firewall-takeover-vulnerabilities

[3] https://www.horizon3.ai/attack-research/palo-alto-expedition-from-n-day-to-full-compromise/