Palo Alto Vulnerability Actively Exploited

Overview

The Cybersecurity and Infrastructure Security Agency (CISA) has issued an alert for a critical vulnerability in Palo Alto Networks' Expedition migration tool, tracked as CVE-2024-5910 (CVSS 9.3). Although this flaw was patched in July 2024, it has recently begun to be actively exploited.

The vulnerability stems from missing authentication mechanisms within the migration tool and could allow an attacker to takeover accounts, gain access to configuration secrets, and gain access to sensitive data.

The flaw can be exploited by sending a simple request to an exposed endpoint to reset the admin password. CVE-2024-5910 impacts versions of the Palo Alto Networks Expedition migration tool below 1.2.92. Upon investigation, researchers found other weaknesses within the same tool:

- CVE-2024-9464: An authenticated command injection
- CVE-2024-9465: An unauthenticated SQL injection
- CVE-2024-9466: Cleartext credentials in logs

Additionally, CVE-2024-5910 can be chained with CVE-2024-9464, which could allow for arbitrary command execution. Due to there being a public PoC and active exploitation, Aspire recommends patching as soon as possible.

Aspire Protects

- **Patch –** Update Expedition to version 1.2.92 or newer. You may find patch guidance in Palo Alto's advisory.
- Confirm that the Expedition installation is not exposed to the internet, as this is unnecessary and increases risk.
- Update all Expedition usernames, passwords, and API keys, along with any firewall credentials managed by the Expedition tool, to prevent unauthorized access.

IoCs

- Security researcher Zach Hanley has explained how to check for IoCs in his blog post:
    - The file "**/var/apache/log/access.log**" will log HTTP requests and should be inspected for the endpoints abused in these vulnerabilities:
        - **/OS/startup/restore/restoreAdmin.php** – Reset admin credentials
        - **/bin/Auth.php** – Authenticate with reset admin credentials
        - **/bin/CronJobs.php** – Insert malicious SQL data for command injection
        - **/bin/configurations/parsers/Checkpoint/CHECKPOINT.php** – Unauthenticated SQL injection to exfiltrate database data

TTPs to Watch

Initial Access

- Exploit Public-Facing Application (T1190) – Attackers may gain access through exposed Expedition endpoints.

Privilege Escalation

- Abuse Elevation Control Mechanism (T1548.002) – Threat actors could escalate privileges by exploiting the missing authentication control.

Credential Access

- OS Credential Dumping (T1003) – Attackers may attempt to access stored credentials within Expedition for lateral movement.

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors. Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyberattacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

Palo Alto Expedition: From N-Day to Full Compromise | Horizon3.ai

CISA Adds Four Known Exploited Vulnerabilities to Catalog | CISA

CVE-2024-5910 Expedition: Missing Authentication Leads to Admin Account Takeover