Patch Now - Vulnerabilities in Palo Alto Networks Expedition Tool, Could Lead to Exposed Firewall Credentials

Overview

Palo Alto Networks has released an urgent advisory regarding five critical vulnerabilities discovered in its Expedition tool, which assists with firewall configuration migration. These vulnerabilities allow attackers to compromise sensitive information, including usernames, passwords, and API keys of PAN-OS firewalls, and escalate to full system compromise. Below is a breakdown of the vulnerabilities:

- **CVE-2024-9463 (CVSS 9.9 - Critical)** - OS command injection vulnerability enabling unauthenticated attackers to run arbitrary OS commands as root, resulting in the disclosure of sensitive firewall data.
- **CVE-2024-9464 (CVSS 9.3 - Critical)** - Similar OS command injection vulnerability allowing attackers to gain access to firewall credentials and device configurations.
- **CVE-2024-9465 (CVSS 9.2 - Critical)** - SQL injection vulnerability that exposes Expedition database contents, including password hashes and usernames, while also allowing for file manipulation.
- **CVE-2024-9466 (CVSS 8.2 - High)** - Cleartext storage of sensitive information vulnerability, potentially exposing firewall usernames, passwords, and API keys.
- **CVE-2024-9467 (CVSS 7.0 - High)** - Reflected XSS vulnerability enabling malicious JavaScript execution, potentially leading to session theft via phishing attacks.

Please note that Palo Alto Networks Expedition versions prior to 1.2.96 **are affected**. PAN-OS firewalls, Panorama, Prisma Access, and Cloud NGFW **are unaffected**. While there is no evidence of active exploitation at this time, Aspire strongly recommends applying patches immediately due to the severity of these vulnerabilities and the potential impact of leaving systems unpatched.

Aspire Protects

- **Apply Patches** – Upgrade to Expedition version 1.2.96 or later to patch all vulnerabilities. You may find patch guidance in Palo Altos' security advisory.
- **Credential Rotation** - After updating, rotate all Expedition and PAN-OS firewall credentials.
- **Restrict Access** - Limit Expedition access to authorized users only. If not in use, ensure that the Expedition system is shut down.
- **SQL Injection Indicator** - For CVE-2024-9465, check for potential compromise using the provided SQL command.

IoCs

There are no known IoCs associated with the above vulnerabilities at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

TTPs to Watch

- **Execution (TA0002)**
  - Command and Scripting Interpreter - Unix Shell (T1059.004) – Attackers can exploit OS command injection vulnerabilities (CVE-2024-9463, CVE-2024-9464) to execute arbitrary OS commands on the Expedition system as root.
- **Privilege Escalation (TA0004)**
  - Exploitation for Privilege Escalation (T1068) – Through vulnerabilities such as CVE-2024-9465 (SQL injection), attackers can elevate privileges by accessing sensitive database information and manipulating files on the system.
- **Credential Access (TA0006)**
  - Unsecured Credentials - Cleartext Storage of Sensitive Information (T1552.001) – The cleartext storage vulnerability (CVE-2024-9466) allows attackers to gain access to firewall usernames, passwords, and API keys.
- **Initial Access (TA0001)**
  - Drive-by Compromise - Reflected XSS (T1189) – Exploiting the reflected XSS vulnerability (CVE-2024-9467) enables attackers to inject malicious JavaScript into authenticated users' browsers, potentially stealing session cookies.
- **Collection (TA0009)**
  - Data from Configuration Repository (T1602.001) – The vulnerabilities allow attackers to extract sensitive configuration data from Expedition, including firewall device configurations and API keys.

Aspire's 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 Managed Security Services**
  - Aspire Managed Security Services provide remote security monitoring and device management – 24 hours a day, 7 days a week. By aggregating and correlating security events from across your IT environment, our remote security monitoring service eliminates “noise” and make sense of what really matters.
  - Our managed security portfolio includes:
    - Managed Firewall
    - Managed IDS/IPS
    - Security event monitoring & incident management
    - Managed Cisco ISE (Identity Services Engine)
    - Endpoint Protection

Supporting Documentation

PAN-SA-2024-0010 Expedition: Multiple Vulnerabilities in Expedition Lead to Exposure of Firewall Credentials (paloaltonetworks.com)

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