Zero-Day Exploits in Palo Alto Networks Firewalls

Overview

Palo Alto Networks has disclosed the exploitation of two zero-day vulnerabilities (CVE-2024-0012 and CVE-2024-9474) affecting its next-generation firewalls. These vulnerabilities allow unauthenticated attackers to gain administrative access and escalate privileges on affected systems.

Authentication Bypass Vulnerability CVE-2024-0012 (CVSS 9.3)

There is a missing authentication for a critical function in PAN-OS that allows for unauthenticated network-based attackers to access the management web interface and gain PAN-OS administrator privileges. This allows the attacker to tamper with configurations and allows the exploitation of other vulnerabilities.

Impacted versions include PAN-OS 10.2, 11.0, 11.1, 11.2 (PA-Series, VM-Series, CN-Series firewalls, Panorama).

Privilege Escalation Vulnerability CVE-2024-9474 (CVSS 6.9)

This privilege escalation vulnerability allows a PAN-OS administrator with access to the management web interface to perform actions with root privileges.

Impacted versions include PAN-OS 10.1, 10.2, 11.0, 11.1, 11.2.

Palo Alto Networks is continuing its investigation into ongoing attacks that leverage both vulnerabilities to target "a limited number of device management web interfaces." The company has reported observing threat actors deploying malware and executing commands on compromised firewalls, warning that **a chained exploit** may already be in use.

Also, Shadowserver is monitoring the number of compromised Palo Alto Networks firewalls and has reported that around 2,000 devices have been breached since the onset of this ongoing campaign. Both vulnerabilities have been added to CISA's Known Exploited Vulnerabilities catalog and federal agencies have until December 9, 2024, to patch their firewalls.

Aspire Protects

- **Patch**
  - CVE-2024-0012
    - Palo Alto has released patch guidance for this vulnerability. Aspire recommends following the guidance to protect your devices.
    - The issue is fixed in PAN-OS 10.2.12-h2, PAN-OS 11.0.6-h1, PAN-OS 11.1.5-h1, PAN-OS 11.2.4-h1, and all later PAN-OS versions.
  - CVE-2024-9474
    - Palo Alto has released patch guidance for this vulnerability. Aspire recommends following the guidance to protect your devices.
    - This issue is fixed in PAN-OS 10.1.14-h6, PAN-OS 10.2.12-h2, PAN-OS 11.0.6-h1, PAN-OS 11.1.5-h1, PAN-OS 11.2.4-h1, and all later PAN-OS versions.
  - Palo Alto also recommends securing your management interface and following their best practices for deployment and access control.

TTPs to Watch

Initial Access

- Exploit Public-Facing Application (T1190).

Privilege Escalation

- Abuse Elevation Control Mechanism (T1548.002).

IoCs

A complete list of IoCs can be found in Palo Alto's GitHub repository.

Targeted Industries

- Healthcare
- Financial Services
- Government and Public Sector
- Technology and Telecommunications
- Critical Infrastructure
- Retail and E-commerce

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

Administrative Access Best Practices

CVE-2024-9474 PAN-OS: Privilege Escalation (PE) Vulnerability in the Web Management Interface

CVE-2024-0012 PAN-OS: Authentication Bypass in the Management Web Interface (PAN-SA-2024-0015)

Threat Brief: Operation Lunar Peek, Activity Related to CVE-2024-0012 and CVE-2024-9474 (Updated Nov. 22)

Unit42-Threat-Intelligence-Article-Information/2024-November-IOC-updates-OperationLunarPeek.txt at main · PaloAltoNetworks/Unit42-Threat-Intelligence-Article-Information · GitHub