Palo Alto PAN-OS Firewall Vulnerability Allows Root-Level Command Execution

***Author**: Portia S. Cole – CTI Researcher*

TL;DR

Palo Alto Networks has released security updates to address CVE-2026-0273, a command injection vulnerability that allows authenticated administrators to execute arbitrary commands as the root user on affected PAN-OS devices.

Two additional vulnerabilities, CVE-2026-0272 and CVE-2026-0269, could allow privilege escalation and firewall service disruption. While no active exploitation has been reported, organizations using affected Palo Alto firewalls and Panorama management appliances should patch immediately.

Overview

There is a command injection vulnerability (CVE-2026-0273, CVSS 6.1) affecting Palo Alto's PAN-OS, the operating system used by Palo Alto Networks PA-Series firewalls, VM-Series virtual firewalls, and Panorama management appliances.

These products are commonly used to inspect and control network traffic, enforce security policies, support VPN and remote access services, and provide centralized firewall management. An attacker with administrative access to an affected device could execute commands as the root user.

Affected Products

- PAN-OS 12.1 prior to fixed releases 12.1.4-h7 and 12.1.7
- PAN-OS 11.2 prior to fixed releases 11.2.4-h18, 11.2.7-h16, 11.2.10-h9, and 11.2.12
- PAN-OS 11.1 prior to fixed releases 11.1.4-h34, 11.1.6-h33, 11.1.7-h7, 11.1.10-h27, 11.1.13-h7, and 11.1.15
- PAN-OS 10.2 prior to fixed releases 10.2.7-h35, 10.2.10-h37, 10.2.13-h22, 10.2.16-h8, and 10.2.18-h7
- PA-Series Firewalls
- VM-Series Virtual Firewalls
- Panorama (M-Series and Virtual Appliances)

Not Affected

- Prisma Access
- Cloud NGFW

CVE-2026-0273 allows an authenticated administrator with access to the PAN-OS command-line interface (CLI) or web management interface to execute operating system commands as the root user. This could give an attacker full control of an affected firewall or Panorama appliance.

Palo Alto Networks also patched CVE-2026-0272, which could allow an authenticated administrator to perform actions with root privileges, and CVE-2026-0269, which could cause affected firewalls to repeatedly reboot. Palo Alto Networks is not aware of any active exploitation.

Aspire Protects

- Patch - Upgrade affected PAN-OS devices to a fixed release.
- Restrict access to the PAN-OS web management interface to trusted internal IP addresses only.
- Limit CLI access to authorized administrators only.
- If available, enable Threat Prevention signatures 510028 and 510029 to help detect and block exploitation attempts.
- Organizations running unsupported PAN-OS versions should upgrade to a supported release.

TTPs

Privilege Escalation

- Exploitation for Privilege Escalation (T1068) – Authenticated administrators may perform actions with root privileges on affected devices.

Execution

- Command and Scripting Interpreter (T1059) – Arbitrary operating system commands may be executed through vulnerable management interfaces.

Endpoint Denial of Service

- Endpoint Denial of Service (T1499) – CVE-2026-0269 may cause repeated firewall reboots, impacting VPN and remote access availability.

IoCs

There are no known IoCs 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.

Targeted Industries

Organizations using affected Palo Alto firewalls or Panorama appliances may be impacted, including those in the following sectors:

- Education
- Energy
- Finance
- Healthcare
- Legal
- Manufacturing
- Public Sector
- Retail

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 cyber attacks.
- **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

CVE-2026-0273 PAN-OS: Authenticated Admin Command Injection Vulnerability via CLI or Web UI