Palo Alto Networks Addresses PAN-OS Command Injection Vulnerability

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

TL;DR

Palo Alto Networks has released security updates for CVE-2026-0273 (CVSS 8.6), an authenticated command injection vulnerability affecting PAN-OS.

Successful exploitation allows an authenticated administrator with access to the CLI or Web UI to execute arbitrary commands as the root user. Palo Alto Networks has not observed exploitation in the wild.

Overview

There is a medium-severity vulnerability (CVE-2026-0273, CVSS 8.6) in Palo Alto Networks PAN-OS that allows an authenticated administrator to bypass system restrictions and execute arbitrary operating system commands with root privileges through the CLI or Web UI.

Affected Products

- PAN-OS 10.2
- PAN-OS 11.1
- PAN-OS 11.2
- PAN-OS 12.1
- PA-Series Firewalls
- VM-Series Firewalls
- Panorama (Virtual and M-Series)

Not Affected

- Cloud NGFW
- Prisma Access

If exploited, an attacker with administrator access could execute arbitrary commands as the root user, allowing them to modify firewall configurations, disable security controls, create persistent access, intercept or redirect network traffic, or use the compromised firewall to carry out additional attacks within the environment.

Aspire Protects

- Upgrade PAN-OS to a supported fixed version. See Palo Alto's advisory for more information.
- Restrict management interface access to trusted internal IP addresses.

- Limit CLI and Web UI access to authorized administrators.
- Require administrators to connect through a secured jump host.
- Enable Threat Prevention signatures 510028 and 510029 where applicable.

TTPs

Execution

- Command and Scripting Interpreter: Unix Shell (T1059.004) – An authenticated administrator can execute arbitrary operating system commands as the root user through the PAN-OS CLI or Web UI.

Privilege Escalation

- Exploitation for Privilege Escalation (T1068) – An authenticated administrator can bypass system restrictions to obtain root-level privileges on the affected firewall or Panorama appliance.

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

Any organization using affected Palo Alto Networks firewalls or Panorama appliances, including:

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

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