# Firewall Management Interfaces Targeted via PHP Flaws in PAN-OS



Palo Alto Networks confirmed on October 28 that attackers are exploiting two PHP vulnerabilities against internet-exposed PAN-OS management interfaces, allowing unauthenticated code execution on the web server.

- Palo Alto Networks confirmed active exploitation on October 28.
- The flaws are CVE-2026-109618 and CVE-2026-109619, both in PHP.
- The target is PAN-OS management interfaces exposed to the internet.
- Both flaws allow code execution on the web server without authentication.
- The source describes the firewall as an early target of PHP2Shell exploitation and notes the disclosure did not go smoothly.

## What was reported

According to The Hacker News, one of the early targets of PHP2Shell exploitation was the firewall. On October 28, Palo Alto Networks confirmed that attackers were exploiting two PHP vulnerabilities, **CVE-2026-109618** and **CVE-2026-109619**, against PAN-OS management interfaces that are reachable from the internet.

Both flaws allow anyone to execute code on the web server without authenticating. The source also notes that the disclosure itself went somewhat wrong, but it gives no further detail in the excerpt available.

## Why it matters

Security devices are often treated as protective layers rather than as web applications. The report's point is that a firewall's management interface is itself a web application, and when it is exposed to the internet it carries the same risks as any other web-facing system. Unauthenticated code execution on such a device is a serious position for an attacker to hold.

## What to do next

The source excerpt does not list patches, affected versions or mitigations, so teams should rely on the vendor's own advisory for those details. In the meantime, the practical priority is to establish whether any PAN-OS management interface in your estate can be reached from the internet, and to treat any such exposure as urgent.

## What to do now

1. Identify every PAN-OS device and check whether its management interface is reachable from the internet.
2. Restrict management access to internal or dedicated management networks and approved administrator addresses.
3. Review the Palo Alto Networks advisory for CVE-2026-109618 and CVE-2026-109619 and apply its guidance.
4. Check management interface and system logs for unexpected activity, and escalate through incident response if found.
5. Include firewall and other security device management interfaces in web application exposure reviews.