Palo Alto Networks patches Fragnesia flaw used to root PAN-OS firewalls



Palo Alto Networks released PAN-OS updates for CVE-2026-46300 (Fragnesia), which attackers chained with PHP2Shell against firewalls whose management interfaces were exposed to the internet.

- CVE-2026-46300 (Fragnesia) is a Linux kernel privilege escalation flaw in the XFRM ESP-in-TCP subsystem, disclosed in May 2026.
- Attackers chained PHP2Shell for remote code execution with Fragnesia to deploy webshells with root privileges.
- Palo Alto Networks confirmed attacks on PAN-OS firewalls with internet-exposed management interfaces.
- PHP2Shell patches have been available for all supported PAN-OS versions since October 30; new

builds now address Fragnesia as well.

- The vendor advises blocking direct internet access to the management interface.

Palo Alto Networks has announced PAN-OS updates that fix CVE-2026-46300, known as Fragnesia, a Linux kernel flaw that has been used to gain root control of its firewalls.

What happened

Fragnesia was disclosed in May 2026 as a privilege escalation bug in the kernel's XFRM ESP-in-TCP subsystem. It lets an unprivileged attacker overwrite sensitive system files and obtain root permissions.

The security firm Dream reported on October 26 that a Chinese-speaking threat actor used the critical PHP2Shell bugs together with Fragnesia in an AI-assisted campaign. According to the report, 25 servers were compromised, 24 firewalls and one internal firewall management server. PHP2Shell gave remote code execution, and the Fragnesia exploit was then used to deploy webshells with root privileges. On October 29, Palo Alto Networks confirmed that PAN-OS firewalls with internet-exposed management interfaces were hit this way.

Patch status

By October 30, fixes for PHP2Shell were available for all supported PAN-OS versions, closing the known initial-access path. The company says that running a fixed version listed in the PHP2Shell advisory provides protection. It has nevertheless released further builds for Fragnesia across the 12.2, 12.1, 11.2, 11.1 and 10.2 branches, and recommends applying them. The only known way to exploit Fragnesia against PAN-OS is to first exploit PHP2Shell through an exposed management interface.

Management interface exposure

Palo Alto Networks advises against direct web access to the management interface. Access should come only from a management network or through a VPN.

What to do now

1. Inventory all PAN-OS firewalls and confirm whether any management interface is reachable from the internet.
2. Restrict management access to a dedicated management network or a VPN.
3. Confirm the PHP2Shell fixes are installed, then apply the PAN-OS build for CVE-2026-46300 on your branch.
4. Review firewalls that had exposed management interfaces for unexpected webshells or file changes, and escalate suspected compromise through incident response.

5. Record the exposure and remediation in your vulnerability management and change records for regulator review.