

**Palo Alto Networks firewall or GlobalProtect VPN environments are part of this security alert.****What is the Issue?**

A security flaw (CVE-2026-0257) has been discovered in Palo Alto Networks PAN-OS, the software that runs the firewall and GlobalProtect VPN. Attackers are actively exploiting this vulnerability right now. This flaw allows an unauthorized person to bypass login security and connect to VPN without valid credentials. This vulnerability has been confirmed by the U.S. Cybersecurity and Infrastructure Security Agency (CISA) as actively exploited in the wild.

You may be affected if your organization uses:

- Palo Alto Networks next-generation firewalls running PAN-OS
- GlobalProtect VPN (portal or gateway components)

Affected products must have the authentication override feature enabled in either the GlobalProtect portal or gateway, and must reuse the authentication override cookie encryption and decryption certificate with another feature in order to be vulnerable.

More information regarding this issue can be found on the links below.

- [Threat Brief: Active Exploitation of PAN-OS CVE-2026-0257](#)
- [CVE-2026-0257 PAN-OS: GlobalProtect Authentication Bypass Vulnerabilities](#) - Palo Alto Networks
- [Rapid7 Observed Exploitation of PAN-OS GlobalProtect Authentication Bypass Vulnerability \(CVE-2026-0257\)](#) - Rapid7
- [Known Exploited Vulnerabilities Catalog](#) - U.S. Cybersecurity & Infrastructure Security Agency (CISA)

What do you need to do?

- PATCH OR UPDATE: Apply the patch released by Palo Alto Networks as soon as possible. If patching cannot be done immediately, workarounds/mitigations are available. As a mitigation, affected products should either disable the authentication override feature or generate a new certificate to use exclusively for the authentication override feature.

What is CloudWave doing?

- For customers that send their Palo Alto logs to our 24/7 SOC, we have reviewed the SIEM for any IoCs and have not found any based on the links provided by Palo and Rapid7

If you have infrastructure support with CloudWave and need assistance assessing your exposure or applying the patch, please contact us at 855-286-7787 or open a Service Request through the Customer Support Portal.