Palo Alto Firewall Authentication Bypass Vulnerability Actively Exploited in the Wild

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

TL;DR

Palo Alto Networks has confirmed active exploitation of CVE-2026-0257 (CVSS 9.1), an authentication bypass vulnerability affecting certain Palo Alto Networks firewalls configured with GlobalProtect VPN services.

Successful exploitation may allow a threat actor to establish unauthorized VPN connections and gain access to internal network resources without valid credentials.

Overview

There is confirmed active exploitation of CVE-2026-0257 (CVSS 9.1), an authentication bypass vulnerability that affects Palo Alto Networks PAN-OS firewalls configured with GlobalProtect Portal or Gateway services. The vulnerability may allow a remote attacker to bypass authentication controls and establish unauthorized VPN connections when Authentication Override cookies are enabled, and a specific certificate configuration is present.

Affected Products

- Palo Alto Networks firewalls running PAN-OS 10.2 prior to 10.2.18-h6
- Palo Alto Networks firewalls running PAN-OS 11.1 prior to 11.1.15
- Palo Alto Networks firewalls running PAN-OS 11.2 prior to 11.2.12
- Palo Alto Networks firewalls running PAN-OS 12.1 prior to 12.1.7
- Prisma Access 10.2 prior to 10.2.10-h36
- Prisma Access 11.2 prior to 11.2.7-h13

The vulnerability affects deployments where

- GlobalProtect Portal or Gateway is configured
- Authentication Override cookies are enabled
- A vulnerable certificate configuration exists

Not Affected

- Panorama
- Cloud NGFW

According to Rapid7, attackers used forged authentication override cookies to authenticate to vulnerable GlobalProtect gateways. In several cases, attackers successfully established VPN access to internal networks through affected firewalls. The Cybersecurity and Infrastructure Security Agency (CISA) added the vulnerability to its Known Exploited Vulnerabilities (KEV) Catalog. Organizations that rely on

GlobalProtect for remote access should patch immediately. Successful exploitation may provide a threat actor with a direct path into internal network resources without requiring valid credentials.

Aspire Protects

- **Patch** - Upgrade affected PAN-OS and Prisma Access deployments to a fixed version immediately. See Palo Alto's security advisory for more information.
- Review GlobalProtect Portal and Gateway configurations for Authentication Override settings.
- Disable Authentication Override cookies if the feature is not required.
- Configure a dedicated certificate exclusively for Authentication Override cookies.
- Review VPN authentication logs for unusual login activity.
- Investigate unauthorized or unexpected VPN sessions.
- Monitor for VPN connections originating from unfamiliar IP addresses.
- Verify all internet-facing Palo Alto Networks firewalls are running supported software versions.

TTPs to Watch

Initial Access

- Exploit Public-Facing Application [T1190] – The attacker may exploit a vulnerable internet-facing GlobalProtect Portal or Gateway to bypass authentication controls and gain unauthorized access.

Initial Access

- External Remote Services [T1133] – The attacker may establish an unauthorized VPN connection to access internal network resources after successfully exploiting the vulnerability.

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 Palo Alto Networks GlobalProtect VPN services may be affected.

- 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-2026-0257 PAN-OS: GlobalProtect Authentication Bypass Vulnerabilities

NVD - CVE-2026-0257

Rapid7 Observed Exploitation of PAN-OS GlobalProtect Authentication Bypass Vulnerability (CVE-2026-0257)