Palo Alto Networks Fixes High-Severity GlobalProtect Vulnerability

TL;DR

Palo Alto Networks patched seven vulnerabilities across its product line, including a high-severity flaw (CVE-2025-4232, CVSS 8.5) in GlobalProtect for macOS that allows local users to gain root access.

PAN-OS command injection bugs (CVSS 7.2 and 6.5) and other privilege escalation issues were also resolved. No exploitation has been reported, but administrators should patch immediately, especially on macOS endpoints and firewalls.

Overview

This week, Palo Alto Networks released patches for seven vulnerabilities across its product line, including a flaw in its GlobalProtect app for macOS. The most impactful vulnerability, CVE-2025-4232 (CVSS 8.5), allows a local, authenticated user to escalate privileges to root due to improper neutralization of wildcards in the log collection component. No special configuration is required for exploitation.

Other patched vulnerabilities include two separate command injection bugs (CVE-2025-4230, CVSS 7.2 and CVE-2025-4231, CVSS 6.5) in PAN-OS, both of which allow privilege escalation to root when exploited by authenticated administrators via the CLI or web interface. Additional flaws patched include insecure packet transmission over SD-WAN, a privilege assignment issue in Cortex XDR Broker VM, and improper access control in GlobalProtect's Endpoint Traffic Policy Enforcement for Windows and macOS.

Affected Products (CVE-2025-4232)

- GlobalProtect App for macOS – Versions 6.0.x, 6.1.x, 6.2.x < 6.2.8-h2, and 6.3.x < 6.3.3
- PAN-OS – Versions supporting web interface and CLI-based administrative access
- Cortex XDR Broker VM – Incorrect privilege assignment
- GlobalProtect Endpoint Traffic Policy – Affects macOS and Windows builds

Palo Alto also integrated 11 recent Chrome security fixes into Prisma Access Browser, including one vulnerability tracked as CVE-2025-4233 (CVSS 8.6). Privilege escalation bugs in remote access tools like GlobalProtect create an easy path to full control. If you have a macOS, patch immediately.

Aspire Protects

- **Patch –** Users should patch immediately. Please see Palo Alto Network's advisory for patch guidance.
    - CVE-2025-4232
        - Upgrade GlobalProtect macOS clients to 6.3.3 or 6.2.8-h2 when available.
        - Apply the latest PAN-OS patches; restrict CLI/web admin access to trusted users only.
        - Patch Cortex XDR Broker VMs and Prisma Access Browser builds.
        - Audit all devices for unexpected root-level actions or privilege shifts.
    - CVE-2025-4231 – Please see Palo Alto Network's advisory for patch guidance.
    - CVE-2025-4230 – Please see Palo Alto Network's advisory for patch guidance.
    - CVE-2025-4233 - Please see Palo Alto Network's advisory for patch guidance.

TTPs to Watch

Initial Access

- Valid Accounts T1078 – The attacker may use stolen or authorized user credentials to log into a macOS system running a vulnerable version of GlobalProtect.

Privilege Escalation

- Exploitation for Privilege Escalation T1068 – The attacker may exploit the wildcard injection flaw in GlobalProtect to escalate privileges from a local user to root.

Execution

- Command and Scripting Interpreter: Unix Shell T1059.004 (macOS/Linux Bash) – Once elevated, the attacker may execute arbitrary commands with root privileges using the macOS shell.

IoCs

There are no known IoCs associated with the above vulnerabilities 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

These vulnerabilities are most concerning for sectors that depend on Palo Alto's firewall, remote access, and endpoint tools to support distributed teams, sensitive data, and critical infrastructure.

- Healthcare
- Financial Services
- Government & Public Sector
- Education
- Manufacturing
- Legal & Professional Services
- 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

PAN-SA-2025-0011 Chromium and Prisma Access Browser: Monthly Vulnerability Update (June 2025)

CVE-2025-4232 GlobalProtect: Authenticated Code Injection Through Wildcard on macOS

NVD - CVE-2025-4232

CVE-2025-4232 GlobalProtect: Authenticated Code Injection Through Wildcard on macOS

CVE-2025-4231 PAN-OS: Authenticated Admin Command Injection Vulnerability in the Management Web Interface

CVE-2025-4230 PAN-OS: Authenticated Admin Command Injection Vulnerability Through CLI