CYBER ADVISORY

TLP:CLEAR

27 February 2025

Active Exploitation of PAN-OS Vulnerabilities

Palo Alto Networks | Exploited in the wild | POC | Chained Vulnerabilities

The California Cybersecurity Integration Center (Cal-CSIC) has identified ongoing exploitation of multiple vulnerabilities leveraged against Palo Alto Networks PAN-OS products, With the most recent vulnerability, CVE-2025-0110, containing a CVSS 3 score of 7.2. This vulnerability, when chained with CVE-2025-0108, CVE-2024-0111, CVE-2024-9474, allows an attacker to gain root access and ultimately perform root privilege actions on the firewall. These root privilege actions include reconfiguring firewalls, exfiltrating sensitive data, or deploying persistent backdoors.[1] Furthermore, Google researchers have released a Proof-of-Concept of this attack chain.[2] These vulnerabilities are recognized in CISA's Known Exploited Vulnerabilities Catalog (KEV) and by Palto Alto.[3]

Additional details on the three above vulnerabilities that are chained with CVE-2025-0110 can be found in Cal-CSIC's advisory titled "Chained Vulnerabilities Exploit Privilege Escalation in PAN-OS" (CAL-CSIC-202502-004).

The Cal-CSIC recommends immediately applying the appropriate updates provided by Palo Alto Networks to vulnerable systems.

For more information on applying the security updates please refer to the PAN-OS Upgrade Guide

Organization, Source, Reference, and Dissemination Information

Organization Description	California Government Code § 8586.5 established the California Cybersecurity Integration Center (Cal-CSIC) as the central organizing hub of state government's cybersecurity activities, including information sharing, intelligence analysis, incident response, and overarching cybersecurity strategy. The Cal-CSIC is responsible for reducing the likelihood and severity of cyber incidents that could damage California's economy, critical infrastructure, and public or private sector networks in our state.

Customer Feedback	If you need further information about this issue, contact the Cal-CSIC at our email address CalCSIC@caloes.ca.gov or by telephone at (833) REPORT1.
Source Summary Statement	This report was compiled from a variety of sources, predominately open-source reporting.
Handling Caveats	**Traffic Light Protocol (TLP):** Recipients may share TLP:CLEAR information with the world; there is no limit on disclosure. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

[1] Cyber Security News; "Google Released PoC Exploit For Palo Alto Firewall Command Injection Vulnerability" https://cybersecuritynews.com/palo-alto-networks-warns-hackers-combining-vulnerabilities/; accessed 26 February 2025

[2] GitHub; "PaloAlto OpenConfig Plugin: Command Injection Vulnerability" https://github.com/google/security-research/security/advisories/GHSA-73px-m3vw-mr35; accessed 26 February 2025

[3] CISA; "Known Exploited Vulnerabilities Catalog" https://www.cisa.gov/known-exploited-vulnerabilities-catalog; accessed 26 February 2025