VULNERABILITY BULLETINS

Palo Alto Patches Two High-Severity Flaws (CVE-2025-0108, CVE-2025-0110)

TLP:WHITE

Feb 13, 2025

On February 12, 2025, Palo Alto Networks published 10 security advisories patching two high-severity vulnerabilities, tracked as CVE-2025-0108 and CVE-2025-0110, along with several other less severe flaws.

CVE-2025-0108 is a PAN-OS flaw that allows unauthenticated attackers with network access to bypass authentication, potentially compromising the integrity and confidentiality of the system. The flaw could also lead to remote code execution when chained with other flaws. The flaw has a CVSS score of 7.8.

The second notable vulnerability, CVE-2025-0110, is a command injection flaw requiring admin privileges. It affects the PAN-OS OpenConfig Plugin and has a CVSS score of 7.3

The remaining flaws addressed in advisories are medium-severity issues in the Cortex XDR agent, Cortex XDR Broker, and PAN-OS.

There are no known active exploitations, but Health-ISAC strongly recommends that these vulnerabilities be patched urgently. To enhance the security of Palo Alto devices, it is also highly advisable to disable access to the management interface from the internet or any untrusted network. These precautions are particularly important

given the widespread use of Palo Alto devices and their frequent targeting by threat actors.

Recommendations:

- Apply available patches for vulnerable Palo Alto Networks devices.
- Disable access to the management interface from the internet or any untrusted network.
- Ensure all of the devices are patched in a timely manner.
- Enforce network segmentation and strict network access control policies.
- Continuously monitor suspicious activities.
- Have an incident response plan ready to limit operational disruptions in the event of a successful attack.
- Review the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients resources.

Reference(s)	The Hacker News, HHS, Palo Alto Networks, Security Week

Sources
https://security.paloaltonetworks.com/
https://www.securityweek.com/palo-alto-networks-patches-potentially-serious-firewall-vulnerability/
https://thehackernews.com/2025/02/palo-alto-networks-patches.html

Release Date
Feb 13, 2025 (UTC)

Alert ID c6433ae0

View Alert

Share Feedback
was this helpful? |

Tags CVE-2025-0110, CVE-2025-0108, Palo Alto Networks

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Access the Health-ISAC Threat Intelligence Portal
Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments
Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.  

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**