CVE-2025-0108 & CVE-2025-0110

Authentication Bypass & Command Injection (Palo Alto Networks PAN-OS)

Vairav Advisory Report

Date: February 13, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

Palo Alto Networks has disclosed two high-severity vulnerabilities in PAN-OS, affecting the management web interface and the OpenConfig plugin. CVE-2025-0108 is an authentication bypass vulnerability that allows unauthenticated attackers to invoke certain PHP scripts, impacting the integrity and confidentiality of PAN-OS. CVE-2025-0110 is a command injection vulnerability in the OpenConfig plugin, allowing authenticated administrators to execute arbitrary commands.

VULNERABILITY DETAILS

CVE-2025-0108

Description: An authentication bypass vulnerability in PAN-OS enables an unauthenticated attacker with network access to the management web interface to bypass authentication and invoke certain PHP scripts. While this does not allow remote code execution, it can impact the integrity and confidentiality of PAN-OS.

Impact: Unauthorized access, and potential data exposure.

CVSS Score: 8.8 (High)

Risk Explanation: The risk is highest when access to the management interface is allowed from external IP addresses on the internet. Mitigating this risk requires restricting access to only trusted internal IPs.

Alternative CVSS Score (With Restricted Access): 5.9 (Medium)

CVE-2025-0110

Description: A command injection vulnerability in the PAN-OS OpenConfig plugin allows an authenticated administrator with gNMI access to bypass system restrictions and execute arbitrary commands with the privileges of the "_openconfig" user.

Impact: Arbitrary command execution, system manipulation.

CVSS Score: 8.6 (High)

Risk Explanation: The risk is highest when access to the management interface is allowed from external IP addresses on the internet. Mitigating this risk requires restricting access to only trusted internal IPs.

Alternative CVSS Score (With Restricted Access): 7.5 (High)

AFFECTED VERSIONS

CVE-2025-0108 (Authentication Bypass):

- PAN-OS 11.2 (before 11.2.4-h4)
- PAN-OS 11.1 (before 11.1.6-h1)
- PAN-OS 10.2 (before 10.2.13-h3)
- PAN-OS 10.1 (before 10.1.14-h9)

CVE-2025-0110 (Command Injection):

- PAN-OS OpenConfig Plugin versions before 2.1.2

EXPLOIT DETAILS

CVE-2025-0108 can be exploited remotely by attackers with network access to the PAN-OS management web interface. CVE-2025-0110 requires an authenticated administrator with access to the gNMI interface, allowing the execution of arbitrary commands

RECOMMENDED ACTIONS

- Palo Alto Networks has released patches to mitigate these vulnerabilities. Users should update to the latest PAN-OS versions

ADDITIONAL SECURITY MEASURES

- Restrict access to the PAN-OS management interface to trusted internal IP addresses.
- Disable or uninstall the OpenConfig plugin if it is not in use.

REFERENCES

https://security.paloaltonetworks.com/CVE-2025-0110

https://security.paloaltonetworks.com/CVE-2025-0108

https://www.cve.org/CVERecord?id=CVE-2025-0110

https://www.cve.org/CVERecord?id=CVE-2025-0108

https://nvd.nist.gov/vuln/detail/CVE-2025-0108

https://nvd.nist.gov/vuln/detail/CVE-2025-0110

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com