



# **CVE-2025-0111 PANOS AUTHENTICATED FILE READ VULNERABILITY**

---

## **Vairav Advisory Report**

**Date: February 20, 2025**

**Vairav Cyber Threat Intelligence Team**

**Vairav Technology Security Pvt. Ltd.**

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: [mail@vairavtech.com](mailto:mail@vairavtech.com)

## EXECUTIVE SUMMARY

Palo Alto Networks has disclosed two vulnerabilities affecting PAN-OS and Cortex XDR Agent. CVE-2025-0111 is a high-severity authenticated file read vulnerability in PAN-OS that allows an attacker with network access to read files accessible by the “nobody” user. Organizations using affected versions should apply security updates immediately.

## VULNERABILITY DETAILS

### CVE-2025-0111

**Description:** An authenticated attacker with network access to the PAN-OS management web interface can read files from the PAN-OS filesystem accessible by the “nobody” user.

**Impact:** Information disclosure, the potential for further privilege escalation.

**CVSS Score:** 7.1 (High)

## AFFECTED VERSIONS

### PAN-OS:

- 11.2 (before 11.2.4-h4)
- 11.1 (before 11.1.6-h1, before 11.1.2-h18)
- 10.2 (before 10.2.13-h3, 10.2.7-h24, 10.2.8-h21, 10.2.9-h21, 10.2.10-h14, 10.2.11-h12, 10.2.12-h6)
- 10.1 (before 10.1.14-h9)

## EXPLOIT DETAILS

Palo Alto Networks has observed exploit attempts chaining CVE-2025-0108 with CVE-2024-9474 and CVE-2025-0111 against unpatched PAN-OS web management interfaces.

## RECOMMENDED ACTIONS

- Palo Alto Networks has released patches to mitigate these vulnerabilities. Users should upgrade to the latest fixed versions.

## ADDITIONAL SECURITY MEASURES

- Restrict management interface access to trusted internal IP addresses.
- Apply endpoint protection policies and disable unnecessary services.
- Enable audit logging to detect unauthorized file access and security agent tampering.

## REFERENCES

<https://security.paloaltonetworks.com/CVE-2025-0111>

<https://app.opencve.io/cve/CVE-2025-0111>

## 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: [mail@vairavtech.com](mailto:mail@vairavtech.com)

Website: <https://vairavtech.com>