CVE-2025-0116 PAN-OS FIREWALL DENIAL OF SERVICE (DOS) USING A SPECIALLY CRAFTED LLDP FRAME

Vairav CVE Report

Date: March 18, 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 a medium-severity vulnerability (CVE-2025-0116) affecting PAN-OS, the operating system powering their network security appliances. This vulnerability allows an unauthenticated, adjacent attacker to cause a firewall reboot using specially crafted LLDP frames, potentially leading to a denial-of-service (DoS) condition. Organizations relying on PAN-OS should immediately apply security updates or implement recommended mitigations.

VULNERABILITY DETAILS

CVE-2025-0116: PAN-OS Firewall Denial of Service (DoS) Using a Specially Crafted LLDP Frame

Description: This vulnerability arises due to improper handling of specially crafted Link Layer Discovery Protocol (LLDP) frames. If an attacker on an adjacent network sends such frames to a vulnerable firewall, it can trigger an unexpected reboot, potentially disrupting network operations. If repeated, this could force the firewall into maintenance mode, leading to prolonged downtime.

Impact: Unauthenticated attackers can disrupt firewall operations, causing service outages and affecting business continuity.

CVSS Score: 6.8 (Medium)

AFFECTED VERSIONS

PAN-OS versions:

- 11.2.0 through 11.2.4
- 11.1.0 through 11.1.7
- 10.2.0 through 10.2.13
- 10.1.0 through 10.1.14

EXPLOIT DETAILS

Attackers can exploit this flaw by sending specially crafted LLDP frames to a vulnerable PAN-OS firewall with LLDP enabled. The attacker can trigger a firewall reboot if LLDP is enabled on at least one network interface and configured in “transmit-receive” or “receive-

only" mode. Continued exploitation can force the firewall into maintenance mode, requiring manual recovery. No public exploits have been reported yet.

RECOMMENDED ACTIONS

Patch & Upgrade:

- Palo Alto Networks has released fixed versions. Organizations should upgrade to PAN-OS 11.2.5, 11.1.8, 10.2.14, or 10.1.14-h11 as soon as possible.

ADDITIONAL SECURITY MEASURES

- **Disable LLDP**: If LLDP is not required, disable it under Network > LLDP in the web interface.
- **Disable LLDP on Interfaces**: Disable LLDP for specific interfaces under Network > Interfaces > Advanced > LLDP.
- **Set LLDP Mode to Transmit-Only**: If LLDP is needed for advertising purposes, configure it in "transmit-only" mode under Network > Network Profiles > LLDP Profile.

REFERENCES

https://app.opencve.io/cve/CVE-2025-0116

https://security.paloaltonetworks.com/CVE-2025-0116

https://www.cve.org/CVERecord?id=CVE-2025-0116

https://nvd.nist.gov/vuln/detail/CVE-2025-0116

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