Advisory Alert

Alert Number: AAA20250407 **Date:** April 7, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**High**	Access Control Vulnerability
Palo Alto	**Medium**	Denial of Service Vulnerability

Description

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Access Control Vulnerability (CVE-2025-29987)
Description	Dell has released security updates addressing an Access Control vulnerability in Dell PowerProtect Data Domain with Data Domain Operating System. **CVE-2025-29987 -** Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) versions prior to 8.3.0.15 contain an Insufficient Granularity of Access Control vulnerability. An authenticated user from a trusted remote client could exploit this vulnerability to execute arbitrary commands with root privileges. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	DD OS 8.3 - Versions 7.7.1.0 through 8.3.0.10 DD OS 7.13.1 - Versions 7.13.1.0 through 7.13.1.20 DD OS 7.10.1 - Versions 7.10.1.0 through 7.10.1.50 PowerProtect DP Series Appliance (IDPA) - Versions 2.7.6, 2.7.7, and 2.7.8 Disk Library for mainframe DLm8500 - Version 5.4.0.0 Disk Library for mainframe DLm8700 - Version 7.0.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000300899/dsa-2025-139-dell-technologies-powerprotect-data-domain-security-update-for-a-security-vulnerability

Affected Product	**Palo Alto**
Severity	**Medium** - Initial release date **17th March 2025 (AAA20250317)**
Affected Vulnerability	Denial of Service Vulnerability (CVE-2025-0116)
Description	Palo Alto has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2025-0116** - A Denial of Service (DoS) vulnerability in Palo Alto Networks PAN-OS software causes the firewall to unexpectedly reboot when processing a specially crafted LLDP frame sent by an unauthenticated adjacent attacker. Repeated attempts to initiate this condition causes the firewall to enter maintenance mode. Palo Alto advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PAN-OS 11.2 Prior to 11.2.5 PAN-OS 11.1 Prior to 11.1.4-h17 PAN-OS 11.1 Prior to11.1.6-h6 PAN-OS 11.1 Prior to11.1.8 PAN-OS 10.2 Prior to 10.2.10-h17 PAN-OS 10.2 Prior to 10.2.13-h5 PAN-OS 10.2 Prior to 10.2.14 PAN-OS 10.1 Prior to 10.1.14-h11
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.paloaltonetworks.com/CVE-2025-0116

Disclaimer

The information provided are gathered from official service provider's websites and portals. FinCSIRT strongly recommends members to apply security fixes as per the given guidelines, following the organization's patch and change management procedures to protect systems from potential threats.