Advisory Alert

Alert Number: AAA20250404 **Date:** April 4, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Ubuntu	**High**, **Medium**	Multiple Vulnerabilities
Dell	**High**, **Medium**	Multiple Vulnerabilities
IBM	**High**, **Medium**	Multiple Vulnerabilities
Zabbix	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Palo Alto	**Medium**	Denial of Service Vulnerability

Description

Affected Product	**Ubuntu**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-56658, CVE-2021-47119, CVE-2024-56600, CVE-2021-47122, CVE-2021-47483, CVE-2024-56595)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in Ubuntu Linux kernel. These vulnerabilities could be exploited by malicious users to cause memory leak, use-after-free, array-index-out-of-bounds. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 14.04 ESM
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-7415-1

Affected Product	**Dell**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-21853, CVE-2024-21944, CVE-2024-27457, CVE-2023-31342, CVE-2023-31343, CVE-2023-31345, CVE-2024-21924, CVE-2024-21925, CVE-2023-20582, CVE-2023-20581, CVE-2023-52340, CVE-2024-42154, CVE-2024-24852, CVE-2024-36274, CVE-2024-38796, CVE-2024-25571, CVE-2024-37020, CVE-2024-21859, CVE-2024-31155, CVE-2024-39813, CVE-2024-39286, CVE-2024-39279, CVE-2024-28047, CVE-2024-31068)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000303519/dsa-2025-164-security-update-for-dell-vxflex-ready-node-and-powerflex-custom-node-multiple-third-party-component-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000287202/dsa-2025-038-security-update-for-dell-poweredge-server-bios-for-tianocore-edk2-vulnerability • https://www.dell.com/support/kbdoc/en-us/000283929/dsa-2025-042-dell-poweredge-server-security-update-for-intel-ethernet-controllers-adapters-and-intel-processor-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000283897/dsa-2025-041-security-update-for-dell-poweredge-server-for-intel-2025-security-advisories-2025-1-ipu • https://www.dell.com/support/kbdoc/en-us/000283913/dsa-2024-381-security-update-for-dell-poweredge-server-for-intel-2024-security-advisories-2024-4-ipu

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-52798, CVE-2025-25285, CVE-2025-25289, CVE-2025-25290, CVE-2025-27152, CVE-2024-51479, CVE-2025-25288, CVE-2018-6341, CVE-2021-23337)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in IBM Security QRadar Analyst Workflow. These vulnerabilities could be exploited by malicious users to compromise the affected system. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Security QRadar Analyst Workflow 1.0.0 - 2.34.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7230024

Affected Product	**Zabbix**
Severity	**High**, **Medium** , **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-45700, CVE-2024-45699, CVE-2024-42325, CVE-2024-36465, CVE-2024-36469)
Description	Zabbix has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Denial of Service, Cross-Site Scripting, SQL injection. Zabbix advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Zabbix Server, Zabbix Proxy versions 6.0.0-6.0.38, 7.0.0-7.0.9, 7.2.0-7.2.3 Zabbix web interface 6.0.0-6.0.37 , 6.4.0-6.4.20, 7.0.0-7.0.6 Zabbix API 5.0.0-5.0.45, 6.0.0-6.0.37, 7.0.0-7.0.8, 7.2.0-7.2.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.zabbix.com/browse/ZBX-26253 • https://support.zabbix.com/browse/ZBX-26254 • https://support.zabbix.com/browse/ZBX-26258 • https://support.zabbix.com/browse/ZBX-26257 • https://support.zabbix.com/browse/ZBX-26255

Affected Product	**Palo Alto**
Severity	**Medium**
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 10.1 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.