Advisory Alert

Alert Number: AAA20260317 **Date:** March 17, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Ubuntu	**High, Medium**	Multiple Vulnerabilities
IBM	**High, Medium**	Multiple Vulnerabilities
Dell	**Medium**	Information Disclosure Vulnerability

Description

Affected Product	**Ubuntu**
Severity	**High, Medium**
Affected Vulnerability	Multiple Vulnerabilities
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in the kernel of their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Ubuntu advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Ubuntu Versions - 20.04, 22.04, 24.04 and 25.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://ubuntu.com/security/notices/USN-8098-1 • https://ubuntu.com/security/notices/USN-8096-1 • https://ubuntu.com/security/notices/USN-8095-1 • https://ubuntu.com/security/notices/USN-8094-1

Affected Product	**IBM**
Severity	**High, Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-29371, CVE-2025-57753, CVE-2025-13466, CVE-2025-15284)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM WebSphere Hybrid Edition 5.1 • IBM WebSphere Application Server – Versions 8.5 & 9.0 • IBM WebSphere Application Server Liberty – Versions 21.0.0.3 – 26.0.0.2 QRadar Log Source Management App – Versions 1.0.0 - 7.0.13
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7266321 • https://www.ibm.com/support/pages/node/7266324 • https://www.ibm.com/support/pages/node/7258235

Affected Product	**Dell**
Severity	**Medium**
Affected Vulnerability	Information Disclosure Vulnerability (CVE-2024-38798)
Description	Dell has released a security update addressing a vulnerability that exists in their products. **CVE-2024-38798:** EDK2 contains a vulnerability in BIOS where an attacker may cause “Exposure of Sensitive Information to an Unauthorized Actor” by local access. Successful exploitation of this vulnerability will lead to possible information disclosure or escalation of privilege and impact Confidentiality. Dell advises to apply these security fixes at your earliest to protect your 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/000440351/dsa-2026-040-security-update-for-dell-poweredge-server-for-a-tianocore-edk2-vulnerability

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.