Advisory Alert

Alert Number: AAA20260107 **Date:** January 7, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
MariaDB	**High**	Directory Traversal Vulnerability
ASUS	**High**	DLL Hijacking Vulnerability
Veeam	**High**, Medium	Multiple Vulnerabilities
IBM	**High**, Medium, Low	Multiple Vulnerabilities
Red Hat	Medium	Multiple Vulnerabilities
Dell	Medium	Security Update
Joomla	Medium	Multiple Vulnerabilities

Description

Affected Product	**MariaDB**
Severity	**High**
Affected Vulnerability	Directory Traversal Vulnerability (CVE-2025-13699)
Description	MariaDB has released a security update addressing a path traversal vulnerability that exists in their products. **CVE-2025-13699**: This vulnerability allows remote attackers to execute arbitrary code on affected installations of MariaDB. Interaction with the mariadb-dump utility is required to exploit this vulnerability but attack vectors may vary depending on the implementation. The specific flaw exists within the handling of view names. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to execute code in the context of the current user. MariaDB advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	MariaDB versions 11.8.4, 11.4.9, 10.11.15 and 10.6.24
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://mariadb.com/docs/server/security/securing-mariadb/security

Affected Product	**ASUS**
Severity	**High**
Affected Vulnerability	DLL Hijacking Vulnerability (CVE-2025-12793)
Description	ASUS has released a security update addressing a DLL hijacking vulnerability that exists in MyASUS. **CVE-2025-12793**: An uncontrolled DLL loading path vulnerability exists in AsusSoftwareManagerAgent. A local attacker may influence the application to load a DLL from an attacker-controlled location, potentially resulting in arbitrary code execution. ASUS advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	MyASUS versions prior to : • 4.0.52.0 for x64 structure • 4.2.50.0 for Arm structure
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.asus.com/security-advisory

Affected Product	**Veeam**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-55125, CVE-2025-59468, CVE-2025-59469, CVE-2025-59470)
Description	Veeam has released a security update addressing multiple vulnerabilities that exists in Veeam Back and Replication. These vulnerabilities could be exploited by malicious users to cause a Remote Code Execution (RCE) and Privilege Escalation. Veeam advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Veeam Backup & Replication versions earlier and including 13.0.1.180. (Only version 13 builds)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.veeam.com/kb4792

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-61984, CVE-2025-61985, CVE-2025-53057, CVE-2025-53066)
Description	IBM has released a security update addressing multiple vulnerabilities that exists in their products. These vulnerabilities could be exploited by malicious users to cause a Code Execution, Unauthorized Access and Information Disclosure. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Db2 Query Management Facility versions 13.1.1 and 13.1.2 DB2 Query Management Facility for z/OS version 12.2.0.5 AIX versions 7.2 and 7.3 VIOS versions 3.1 and 4.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7256328 • https://www.ibm.com/support/pages/node/7256321 • https://www.ibm.com/support/pages/node/7256323

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-52513, CVE-2024-35868, CVE-2025-39925, CVE-2025-39971)
Description	Red Hat has released a security update addressing multiple vulnerabilities that exists in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Red Hat advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.4 x86_64 Red Hat Enterprise Linux Server - AUS 9.4 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.4 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.4 aarch64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.4 x86_64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.4 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.4 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.4 aarch64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.4 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.4 s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:0173

Affected Product	**Dell**
Severity	**Medium**
Affected Vulnerability	Security Update (CVE-2025-38798)
Description	Dell has released a security update addressing a vulnerability that exists in the third party product INSYDE BIOS that is present in Dell products. **CVE-2025-38798**: Uncleared password keystrokes in circular queue might lead to information disclosure or escalation of privilege. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Dell 14 DC14255 BIOS Versions prior to 1.6.2 Dell 16 DC16255 BIOS Versions prior to 1.4.0 Dell 16 DC16256 BIOS Versions prior to 1.4.0 Dell G15 5535 BIOS Versions prior to 1.17.0 Dell Pro 14 Essential BIOS Versions prior to 1.6.2 Inspiron 14 5445 BIOS Versions prior to 1.16.1 Inspiron 14 7445 2-in-1 BIOS Versions prior to 1.16.1 Inspiron 16 5645 BIOS Versions prior to 1.16.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000412345/dsa-2025-422-security-update-for-dell-client-platform-for-an-insyde-bios-vulnerability

Affected Product	**Joomla**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-63082, CVE-2025-63083)
Description	Joomla has released a security update addressing multiple vulnerabilities that exists in Joomla CMS. **CVE-2025-63082**: Lack of input filtering leads to an XSS vector in the HTML filter code related to data URLs in img tags **CVE-2025-63083**: Lack of output escaping leads to a XSS vector in the pagebreak plugin. Joomla advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Joomla! CMS versions 3.9.0-5.4.1, 4.0.0-5.4.1, and 6.0.0-6.0.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://developer.joomla.org/security-centre/1016-20260101-core-inadequate-content-filtering-for-data-urls.html • https://developer.joomla.org/security-centre/1017-20260102-core-xss-vector-in-the-pagebreak-plugin.html

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.