Advisory Alert

Alert Number: AAA20260127 **Date:** January 27, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SUSE	**High**	Multiple Vulnerabilities
IBM	**High**, Medium	Multiple Vulnerabilities
Red Hat	**High**, Medium	Multiple Vulnerabilities
MariaDB	Medium	Denial of Service Vulnerability

Description

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. SUSE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	openSUSE Leap 15.6 SUSE Linux Enterprise High Availability Extension 15 SP6 SUSE Linux Enterprise Live Patching 15-SP6 SUSE Linux Enterprise Real Time 15 SP6 SUSE Linux Enterprise Server 15 SP6 SUSE Linux Enterprise Server 15 SP6 LTSS SUSE Linux Enterprise Server for SAP Applications 15 SP6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2026/suse-su-20260293-1/

Affected Product	**IBM**
Severity	**High**, Medium
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-21945, CVE-2026-21925)
Description	IBM has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-21945:** Java SE is vulnerable to a denial of service, caused by an easily exploitable vulnerability issue that allows a remote attacker to cause a hang or repeatable crash of the application. **CVE-2026-21925:** Java SE could allow a remote unauthenticated attacker to bypass security controls and perform unauthorized update, insert, delete, or read operations on accessible data, caused by a difficult to exploit vulnerability. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM WebSphere Application Server Version 9.0 IBM WebSphere Application Server Version 8.5 IBM WebSphere Application Server Liberty Continuous delivery version
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7258042

Affected Product	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-21815, CVE-2025-37789, CVE-2025-37761, CVE-2025-37819, CVE-2025-37891, CVE-2025-40154, CVE-2025-40277, CVE-2025-38141, CVE-2025-38349, CVE-2025-38731, CVE-2025-40248, CVE-2025-40258, CVE-2025-40294, CVE-2025-68301, CVE-2025-68305, CVE-2023-53673)
Description	Red Hat has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system Red Hat advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 10.0 aarch64 Red Hat CodeReady Linux Builder for ARM 64 8 aarch64 Red Hat CodeReady Linux Builder for ARM 64 9 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 10.0 s390x Red Hat CodeReady Linux Builder for IBM z Systems 9 s390x Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 10.0 ppc64le Red Hat CodeReady Linux Builder for Power, little endian 8 ppc64le Red Hat CodeReady Linux Builder for Power, little endian 9 ppc64le Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 10.0 x86_64 Red Hat CodeReady Linux Builder for x86_64 8 x86_64 Red Hat CodeReady Linux Builder for x86_64 9 x86_64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 10.0 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 10.0 aarch64 Red Hat Enterprise Linux for ARM 64 8 aarch64 Red Hat Enterprise Linux for ARM 64 9 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 10.0 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 10.0 s390x Red Hat Enterprise Linux for IBM z Systems 8 s390x Red Hat Enterprise Linux for IBM z Systems 9 s390x Red Hat Enterprise Linux for Power, little endian - 4 years of support 10.0 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 10.0 ppc64le Red Hat Enterprise Linux for Power, little endian 8 ppc64le Red Hat Enterprise Linux for Power, little endian 9 ppc64le Red Hat Enterprise Linux for x86_64 - 4 years of updates 10.0 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 10.0 x86_64 Red Hat Enterprise Linux for x86_64 8 x86_64 Red Hat Enterprise Linux for x86_64 9 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:1236 • https://access.redhat.com/errata/RHSA-2026:1143 • https://access.redhat.com/errata/RHSA-2026:1142

Affected Product	**MariaDB**
Severity	**Medium**
Affected Vulnerability	Denial of Service Vulnerability (CVE-2026-21968)
Description	MariaDB has released a security update addressing a denial of service vulnerability that exists in their products. **CVE-2026-21968:** Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. MariaDB advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	MariaDB versions 12.2.2, 11.8.6, 11.4.10 and 10.11.16
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://mariadb.com/docs/server/security/securing-mariadb/security

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.