TLP: WHITE

Advisory Alert

Alert Number: **AAA20260203** **Date:** **February 3, 2026**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Red Hat	**High**, **Medium**	Multiple Vulnerabilities
IBM	**High**, **Medium**	Multiple Vulnerabilities
Node.js	**Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-21863, CVE-2025-40248, CVE-2025-68301, CVE-2024-26766, CVE-2025-38022, CVE-2025-38024, CVE-2025-38415, CVE-2025-38459, CVE-2025-39760, CVE-2025-40258, CVE-2025-40271, CVE-2025-40322, CVE-2022-50865)
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 9.6 aarch64 Red Hat CodeReady Linux Builder for ARM 64 8 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.6 s390x Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.6 ppc64le Red Hat CodeReady Linux Builder for Power, little endian 8 ppc64le Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.6 x86_64 Red Hat CodeReady Linux Builder for x86_64 8 x86_64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.6 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.6 aarch64 Red Hat Enterprise Linux for ARM 64 8 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.6 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.6 s390x Red Hat Enterprise Linux for IBM z Systems 8 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.6 ppc64le Red Hat Enterprise Linux for Power, little endian 8 ppc64le Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.6 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.6 x86_64 Red Hat Enterprise Linux for x86_64 8 x86_64 Red Hat Enterprise Linux Server - AUS 9.6 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.6 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:1703 • https://access.redhat.com/errata/RHSA-2026:1662

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-3517, CVE-2026-1188, CVE-2026-21945, CVE-2026-21925)
Description	IBM has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to conduct Denial of Service (DoS), Buffer Overflow and Authentication Bypass attacks. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM DB2 Data Management Console versions 3.1.9.0 to 3.1.12.0 IBM WebSphere Application Server version 9.0 IBM WebSphere Application Server versions 8.5.0.0 to 8.5.5.28 WebSphere Service Registry and Repository versions 8.5 to 8.5.6.3 IBM WebSphere Application Server - Liberty Continuous delivery
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7259447 • https://www.ibm.com/support/pages/node/7259445 • https://www.ibm.com/support/pages/node/7259422 • https://www.ibm.com/support/pages/node/7258042

Affected Product	**Node.js**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-11187, CVE-2025-69421, CVE-2026-22795)
Description	Node.js has released a security update addressing multiple vulnerabilities that exist in their products. CVE-2025-11187: PBMAC1 parameters in PKCS#12 files are missing validation which can trigger a stack-based buffer overflow, invalid pointer or NULL pointer dereference during MAC verification. The stack buffer overflow or NULL pointer dereference may cause a crash leading to Denial of Service for an application that parses untrusted PKCS#12 files CVE-2025-69421: Processing a malformed PKCS#12 file can trigger a NULL pointer dereference in the PKCS12_item_decrypt_d2i_ex() function. A NULL pointer dereference can trigger a crash which leads to Denial of Service for an application processing PKCS#12 files CVE-2026-22795: An invalid or NULL pointer dereference can happen in an application processing a malformed PKCS#12 file. An application processing a malformed PKCS#12 file can be caused to dereference an invalid or NULL pointer on memory read, resulting in a Denial of Service. Node.js advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	v20.x Branch, Open SSL version 3.0.15 v22.x Branch, Open SSL version 3.5.4 v24.x Branch, Open SSL version 3.5.4 v25.x Branch, Open SSL version 3.5.4 Main Branch, Open SSL version 3.5.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://nodejs.org/en/blog/vulnerability/openssl-fixes-in-regular-releases-jan2026

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.