Advisory Alert

Alert Number: AAA20260309 **Date:** March 9, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
IBM	**High**, **Medium**	Multiple Vulnerabilities
Red Hat	**High**, **Medium**	Multiple Vulnerabilities
Zabbix	**Medium**	Unauthorized Access Vulnerability

Description

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-48910, CVE-2022-46337, CVE-2022-45047, CVE-2023-45133)
Description	IBM has released security updates addressing multiple vulnerabilities that exists in their product. 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 DB2 Data Management Console – Versions 3.1.11 to 3.1.12
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7262753 • https://www.ibm.com/support/pages/node/7262754

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-41909, CVE-2024-21634, CVE-2024-47875, CVE-2023-35887)
Description	IBM has released security updates addressing multiple vulnerabilities that exists in their product. 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 DB2 Data Management Console – Versions 3.1.11 to 3.1.12
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7262753 • https://www.ibm.com/support/pages/node/7262754

Affected Product	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-71085, CVE-2026-23001, CVE-2025-38106, CVE-2025-40248)
Description	Red Hat 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. 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 8 x86_64 Red Hat Enterprise Linux for IBM z Systems 8 s390x Red Hat Enterprise Linux for Power, little endian 8 ppc64le Red Hat Enterprise Linux for ARM 64 8 aarch64 Red Hat CodeReady Linux Builder for x86_64 8 x86_64 Red Hat CodeReady Linux Builder for Power, little endian 8 ppc64le Red Hat CodeReady Linux Builder for ARM 64 8 aarch64 Red Hat Enterprise Linux for x86_64 9 x86_64 Red Hat Enterprise Linux for IBM z Systems 9 s390x Red Hat Enterprise Linux for Power, little endian 9 ppc64le Red Hat Enterprise Linux for ARM 64 9 aarch64 Red Hat CodeReady Linux Builder for x86_64 9 x86_64 Red Hat CodeReady Linux Builder for Power, little endian 9 ppc64le Red Hat CodeReady Linux Builder for ARM 64 9 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems 9 s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:3963 • https://access.redhat.com/errata/RHSA-2026:3966 • https://access.redhat.com/errata/RHSA-2026:3987

Affected Product	**Zabbix**
Severity	**Medium**
Affected Vulnerability	Unauthorized Access Vulnerability (CVE-2026-23925)
Description	Zabbix has released a security update addressing a vulnerability that exists in their product. **CVE-2026-23925**: An authenticated Zabbix user (User role) with template/host write permissions is able to create objects via the configuration.import API. This can lead to confidentiality loss by creating unauthorized hosts. Zabbix advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Zabbix API Versions: • 6.0.0-6.0.40 • 7.0.0-7.0.17 • 7.4.0-7.4.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.zabbix.com/browse/ZBX-27567

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.