Advisory Alert

Alert Number: AAA20260831 **Date:** August 31, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
Red Hat	**High**, **Medium**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
MongoDB	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Vendor	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-10805, CVE-2025-10263, CVE-2026-1933, CVE-2026-3012, CVE-2026-4408, CVE-2026-14474, CVE-2026-33845, CVE-2026-33846, CVE-2026-34982, CVE-2026-42009, CVE-2026-64531, CVE-2025-5222, CVE-2025-40026, CVE-2026-2340, CVE-2026-14476, CVE-2026-35177, CVE-2026-41411, CVE-2026-46483, CVE-2026-48864, CVE-2026-42010, CVE-2026-43329, CVE-2026-5260, CVE-2026-5450, CVE-2026-42011, CVE-2026-42013)
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	• RHEL (base OS) • RHEL for x86_64 – Extended Life Cycle Long Life 8.4 (x86_64) • RHEL Server – AUS 8.4 (x86_64) • OpenShift Container Platform 4.14 — RHEL 8 & 9, all architectures (x86_64, ppc64le, s390x, aarch64) • OpenShift Container Platform 4.15 — RHEL 8 & 9, all architectures (x86_64, ppc64le, s390x, aarch64) • OpenShift Container Platform 4.16 — RHEL 9 only, all architectures (x86_64, ppc64le, s390x, aarch64)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:61239 https://access.redhat.com/errata/RHSA-2026:56786 https://access.redhat.com/errata/RHSA-2026:56853 https://access.redhat.com/errata/RHSA-2026:56911

Vendor	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-10842, CVE-2026-11897, CVE-2026-15057, CVE-2026-14981, CVE-2026-15064, CVE-2026-15328, CVE-2026-15325, CVE-2026-9563, CVE-2025-13465, CVE-2022-50228, CVE-2023-53305, CVE-2025-9900, CVE-2025-62229, CVE-2025-62230, CVE-2025-62231, CVE-2025-11561, CVE-2025-6395, CVE-2025-32988, CVE-2025-32990, CVE-2022-50367, CVE-2023-53178, CVE-2025-40300, CVE-2025-4945, CVE-2025-11021, CVE-2023-53373, CVE-2025-39757, CVE-2026-3686, CVE-2022-50386, CVE-2023-53297, CVE-2023-53386, CVE-2025-39817, CVE-2025-39841, CVE-2025-39849, CVE-2023-53226, CVE-2023-53257, CVE-2025-39864, CVE-2025-38527, CVE-2025-39730, CVE-2025-40778)
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	PowerVM Novalink versions: • 2.2.0, 2.2.1, and 2.2.1.1 • 2.3.0, 2.3.0.1, 2.3.1, 2.3.2, and 2.3.3 IBM Cloud Pak for Data System version 11.3.0.2-IF1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7285568 https://www.ibm.com/support/pages/node/7285507

Vendor	**MongoDB**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-75159, CVE-2026-75573, CVE-2026-81521, CVE-2026-81522, CVE-2026-81523, CVE-2026-81524, CVE-2026-81525, CVE-2026-81526, CVE-2026-81527, CVE-2026-81528, CVE-2026-81529, CVE-2026-81530, CVE-2026-76794, CVE-2026-76797, CVE-2026-76798, CVE-2026-77184, CVE-2026-77586, CVE-2026-81490, CVE-2026-81517, CVE-2026-81518, CVE-2026-81520, CVE-2026-81532, CVE-2026-81533)
Description	MongoDB 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 systems. MongoDB advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	BI Connector versions prior to 2.14.31 GO Driver versions prior to 2.8.2 C++ Driver versions prior to 4.5.1 libmongocrypt versions prior to 1.20.3 C Driver versions prior to 2.5.1 PHP Library versions prior to 2.4.1 PHP Extension versions prior to 2.4.1 Rust Driver versions prior to 3.8.2 C# Driver versions prior to 3.11.1 BI Connector Transition Readiness Report versions prior to 1.1.3 BI Connector ODBC Driver versions prior to 1.4.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.mongodb.com/resources/products/alerts#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.