Advisory Alert

Alert Number: AAA20260707 **Date:** July 7, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

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

Description

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-10109, CVE-2026-3381, CVE-2026-4800, CVE-2026-11707)
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	IBM Db2: versions 11.5.0 - 11.5.9 and 12.1.0 - 12.1.4 QRadar WinCollect versions Agent: 10.0.0 - 10.1.15 IBM WebSphere Hybrid Edition: 5.1 IBM WebSphere Application Server: versions 8.5.5.0 - 8.5.5.29 and 9.0.0.0 - 9.0.5.28
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7277424 • https://www.ibm.com/support/pages/node/7279147 • https://www.ibm.com/support/pages/node/7279199

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-10263, CVE-2026-43112, CVE-2026-43276, CVE-2026-46116, CVE-2026-46155, CVE-2026-46209, CVE-2026-46227, CVE-2026-46244, CVE-2026-46259, CVE-2026-46316, CVE-2026-46323, CVE-2025-71116, CVE-2026-22984, CVE-2026-22990, CVE-2026-23455, CVE-2026-31408, CVE-2026-31669, CVE-2026-43198, CVE-2026-43329, CVE-2026-45852, CVE-2026-46090, CVE-2026-46181, CVE-2026-43279, CVE-2026-45984, CVE-2026-43125, CVE-2026-23270)
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 7 Server (Extended Life Cycle Support): x86_64, s390x, ppc64, ppc64le • Red Hat Enterprise Linux 8.4 (EUS/AUS): x86_64 • Red Hat Enterprise Linux 8.8 (EUS/TUS/SAP): x86_64, ppc64le • Red Hat Enterprise Linux 9 Base & CodeReady Builder: x86_64, aarch64, ppc64le, s390x • Red Hat Enterprise Linux 9.8 (EUS/SAP/4-Year/ELS/CodeReady EUS): x86_64, aarch64, ppc64le, s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:36018 • https://access.redhat.com/errata/RHSA-2026:35896 • https://access.redhat.com/errata/RHSA-2026:35894 • https://access.redhat.com/errata/RHSA-2026:35844 • https://access.redhat.com/errata/RHSA-2026:35863

Vendor	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-11594, CVE-2026-11383, CVE-2026-11806, CVE-2026-11541, CVE-2026-5545, CVE-2025-13465, CVE-2025-14017, CVE-2025-5025, CVE-2025-4947, CVE-2026-33671, CVE-2026-33672, CVE-2026-4873, CVE-2026-6253, CVE-2026-6276, CVE-2026-6429, CVE-2026-7009, CVE-2026-7168, CVE-2026-27171, CVE-2025-36372)
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	• IBM WebSphere Hybrid Edition: 5.1 • IBM WebSphere Application Server Liberty: versions 17.0.0.3 - 26.0.0.6 • IBM WebSphere Application Server: versions 8.5.5.0 - 8.5.5.29 and 9.0.0.0 - 9.0.5.28 • QRadar WinCollect Agent: versions 10.0.0 - 10.1.15 • IBM Db2: versions 11.5.0 - 11.5.9 and 12.1.0 - 12.1.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7279199 • https://www.ibm.com/support/pages/node/7279194 • https://www.ibm.com/support/pages/node/7279196 • https://www.ibm.com/support/pages/node/7279147 • https://www.ibm.com/support/pages/node/7277417

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.