Advisory Alert

Alert Number: AAA20260803 **Date:** August 3, 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
Ubuntu	**High**, Medium, Low	Multiple Vulnerabilities

Description

Vendor	**Red Hat**
Severity	**High**, Medium
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-52923, CVE-2026-52993, CVE-2026-64530, CVE-2026-31692, CVE-2026-43116, CVE-2026-46150, CVE-2025-68211, CVE-2026-46303, CVE-2025-10263, CVE-2026-46113, CVE-2026-46116, CVE-2026-53359, CVE-2025-40026, CVE-2026-63807)
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	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:49212 • https://access.redhat.com/errata/RHSA-2026:49214 • https://access.redhat.com/errata/RHSA-2026:49211 • https://access.redhat.com/errata/RHSA-2026:49033 • https://access.redhat.com/errata/RHSA-2026:49032 • https://access.redhat.com/errata/RHSA-2026:49031 • https://access.redhat.com/errata/RHSA-2026:49030

Vendor	**IBM**
Severity	**High**, Medium, Low
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-54512, CVE-2026-54513, CVE-2026-54514, CVE-2026-54515, CVE-2024-47072, CVE-2025-36442, CVE-2025-36428, CVE-2025-36427, CVE-2025-36424, CVE-2025-36407, CVE-2025-36387, CVE-2025-36366, CVE-2025-36384, CVE-2025-36365, CVE-2025-8916, CVE-2025-58056, CVE-2025-58057, CVE-2025-55163, CVE-2025-36353, CVE-2025-36098, CVE-2025-36123, CVE-2025-36070, CVE-2025-36009, CVE-2025-36001, CVE-2025-36184, CVE-2025-2668, CVE-2025-36122, CVE-2025-14688, CVE-2025-67735, CVE-2025-68161, CVE-2025-12183, CVE-2026-1352, CVE-2026-1577, CVE-2026-3676, CVE-2026-10842, CVE-2026-8053, CVE-2026-8200, CVE-2026-8202, CVE-2026-6914, CVE-2026-6915, CVE-2026-8199, CVE-2026-8201, CVE-2026-41115, CVE-2026-11806, CVE-2026-22016, CVE-2026-22021, CVE-2026-22013, CVE-2026-22018, CVE-2026-34268, CVE-2026-22007, CVE-2025-14914, CVE-2025-66035, CVE-2024-29371, CVE-2026-3621, CVE-2025-14915, CVE-2026-27970, CVE-2026-22610, CVE-2025-14923, CVE-2025-66412, CVE-2025-48924, CVE-2026-1561, CVE-2025-14917, CVE-2025-46392, CVE-2026-5516, CVE-2026-4410, CVE-2026-33814, CVE-2026-39824, CVE-2026-34477, CVE-2026-34478)
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	WebSphere Service Registry and Repository - Versions 8.5 IBM WebSphere Automation - Versions 1.12.0 & 1.12.1 IBM WebSphere Application Server - Versions Liberty 17.0.0.3 - 26.0.0.6 IBM Cloud Pak System Versions: • 2.3.4 • 2.3.5 • 2.3.6 • 2.3.6.1 IBM Cloud Pak System Software - Version 2.3.5.1 IBM Storage Protect for Space Management - Versions 8.1.0.0 - 8.2.1.0 IBM Storage Protect for Virtual Environments: DP for Hyper-V - Versions 8.1.0.0 - 8.2.1.0 IBM Storage Protect for Virtual Environments: DP for VMware - Versions 8.1.0.0 - 8.2.1.0 IBM Storage Protect Client - Version 8.1.0.0 - 8.2.1.0 IBM Storage Protect Operations Center - Version 8.1 & 8.2 IBM Db2 Developer Extension - Version 1.1.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/bulletin/

Vendor	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	Ubuntu 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. Ubuntu advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	20.04 & 22.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://ubuntu.com/security/notices/USN-8620-3 • https://ubuntu.com/security/notices/USN-8620-4

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.