



Advisory Alert

Alert Number: AAA20260928 Date: September 28, 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
Dell	High	Multiple Vulnerabilities
IBM	High, Medium, Low	Multiple Vulnerabilities
Ubuntu	High, Medium, Low	Multiple Vulnerabilities

Description

Vendor	IBM
Severity	Critical
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-58062, CVE-2026-8763, CVE-2026-59650, CVE-2026-29167, CVE-2026-42535, CVE-2026-44631, CVE-2026-68525, CVE-2026-65182, CVE-2026-65905, CVE-2026-64320, CVE-2026-63886, CVE-2026-52924, CVE-2026-68388, CVE-2026-63888, CVE-2026-63887, CVE-2026-53399, CVE-2026-63800, CVE-2026-64018, CVE-2026-64268, CVE-2026-74581, CVE-2025-7783, CVE-2026-29063, CVE-2025-62718, CVE-2026-4800, CVE-2026-42044, CVE-2026-42264, CVE-2026-45623, CVE-2026-13697, CVE-2026-33937, CVE-2026-84961, CVE-2026-48713, CVE-2026-90711, CVE-2026-75604, CVE-2026-42043)
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	Analyst Workflow versions 1.0.0 – 3.1.0 IBM QRadar Pre-Validation App versions 1.0.0 – 2.0.2 IBM QRadar versions: 7.5.0 – 7.5.0 UP16 7.6.0 – 7.6.0.2 IBM Secure Proxy versions 6.1.0.0 – 6.2.1.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7289584 https://www.ibm.com/support/pages/node/7289547 https://www.ibm.com/support/pages/node/7289712 https://www.ibm.com/support/pages/node/7289579 https://www.ibm.com/support/pages/node/7289581

Vendor	Red Hat
Severity	High
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-56171, CVE-2025-5994, CVE-2025-6965, CVE-2025-9230, CVE-2025-9566, CVE-2025-24928, CVE-2025-49794, CVE-2025-49796, CVE-2026-2340, CVE-2026-3012, CVE-2026-3833, CVE-2026-6893, CVE-2026-14164, CVE-2026-15816, CVE-2026-29111, CVE-2026-42010, CVE-2026-43112, CVE-2025-40323, CVE-2026-31539, CVE-2026-46199, CVE-2026-46204, CVE-2026-46230, CVE-2026-46311, CVE-2026-52912, CVE-2026-53203, CVE-2026-53290, CVE-2026-64098, CVE-2026-68108, CVE-2026-68121, CVE-2026-68257, CVE-2026-68266, CVE-2026-68267, CVE-2026-68273, CVE-2026-80714, CVE-2025-39964, CVE-2026-53266, CVE-2026-74581)
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 Platform & Enterprise Software: Red Hat OpenShift Container Platform 4.15 (RHEL 8 / 9): * aarch64, ppc64le, s390x, x86_64 Red Hat Enterprise Linux 9 & 9.8: * Base RHEL 9 & CodeReady Linux Builder 9: aarch64, ppc64le, s390x, x86_64 * 4 Years of Updates: aarch64, s390x * Extended Life Cycle: aarch64, ppc64le, s390x, x86_64 * Extended Update Support (EUS) & CodeReady Linux Builder EUS: aarch64, ppc64le, s390x, x86_64 * Update Services for SAP Solutions: ppc64le, x86_64 Red Hat Enterprise Linux 10: * Base RHEL 10: aarch64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:67857 https://access.redhat.com/errata/RHSA-2026:71700 https://access.redhat.com/errata/RHSA-2026:72059

Vendor	Dell
Severity	High
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-71174, CVE-2026-74777, CVE-2026-74778, CVE-2026-74779, CVE-2026-74780, CVE-2026-74781, CVE-2026-74782, CVE-2026-74805, CVE-2026-74806, CVE-2026-74807, CVE-2026-74808, CVE-2026-74809, CVE-2026-74810, CVE-2026-74811, CVE-2026-74812, CVE-2026-74813, CVE-2026-74814, CVE-2026-74815, CVE-2026-74816, CVE-2026-74817, CVE-2026-74818, CVE-2026-74819, CVE-2026-76106, CVE-2026-76107, CVE-2026-76108, CVE-2026-76109, CVE-2026-20716, CVE-2026-43503, CVE-2026-46331)
Description	Dell 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. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Red Hat OpenShift on Dell Private Cloud Versions prior to 01.04.00.00
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000513460/dsa-2026-440-security-update-for-red-hat-openshift-on-dell-private-cloud-for-multiple-third-party-component-vulnerabilities

Vendor	IBM
Severity	High, Medium, Low
Affected Vulnerability	Multiple Vulnerabilities
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	Analyst Workflow: 1.0.0 – 3.1.0 IBM InfoSphere Optim Archive Viewer: 11.7.0.0 – 11.7.0.14 IBM QRadar: 7.5.0 – 7.5.0 UP16, 7.6.0 – 7.6.0.3 IBM QRadar Pre-Validation App: 1.0.0 – 2.0.2 IBM Secure Proxy: 6.1.0.0 – 6.2.1.2 IBM Security Verify Bridge: 1.0.0.0 – 1.0.17.0 IBM Verify Identity Governance - Container: IVIG 11.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7289712 https://www.ibm.com/support/pages/node/7289515 https://www.ibm.com/support/pages/node/7289484 https://www.ibm.com/support/pages/node/7289510 https://www.ibm.com/support/pages/node/7289579 https://www.ibm.com/support/pages/node/7289581 https://www.ibm.com/support/pages/node/7289547 https://www.ibm.com/support/pages/node/7289584

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	Ubuntu versions 24.04, 20.04, 18.04, 16.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-8729-5 https://ubuntu.com/security/notices/USN-8819-2 https://ubuntu.com/security/notices/USN-8818-2 https://ubuntu.com/security/notices/USN-8730-6

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.