Advisory Alert

Alert Number: AAA20260825 **Date:** August 25, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

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

Description

Vendor	**Red Hat**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Red Hat 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. Red Hat advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Red Hat Update Infrastructure
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:58981

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-44990, CVE-2026-42044, CVE-2026-42043, CVE-2026-48713, CVE-2026-39892)
Description	IBM 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. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM Cloud Pak for Security versions 1.10.0.0 - 1.10.11.0 QRadar Suite Software versions 1.10.12.0 - 1.11.10.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7284670

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-43499, CVE-2026-45984, CVE-2026-46116, CVE-2026-46227, CVE-2026-64531, CVE-2025-40026, CVE-2025-54518, CVE-2026-43125, CVE-2026-46054)
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 8 Base: x86_64, ppc64le • Red Hat Enterprise Linux 8.4 (Advanced Update Support, Extended Life Cycle Long Life): x86_64 • Red Hat Enterprise Linux 8.8 (Extended Life Cycle Long Life, Update Services for SAP Solutions): x86_64, ppc64le • Red Hat Enterprise Linux 8.10 (Extended Life Cycle): x86_64, ppc64le • Red Hat Enterprise Linux 9 Base: x86_64, ppc64le • Red Hat Enterprise Linux 9.2 (Advanced Update Support, Update Services for SAP Solutions, Extended Life Cycle): x86_64, ppc64le • Red Hat Enterprise Linux 9.4 (Advanced Update Support, Update Services for SAP Solutions, Extended Life Cycle): x86_64, ppc64le • Red Hat Enterprise Linux 9.6 (Extended Update Support, Advanced Update Support, Update Services for SAP Solutions, Extended Life Cycle): x86_64, ppc64le • Red Hat Enterprise Linux 9.8 (Extended Update Support, Update Services for SAP Solutions, Extended Life Cycle): x86_64, ppc64le • Red Hat Enterprise Linux 10 Base: x86_64, ppc64le • Red Hat Enterprise Linux 10.2 (Extended Update Support, Four Years of Support/Updates, Extended Life Cycle): x86_64, ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:59142 https://access.redhat.com/errata/RHSA-2026:59143 https://access.redhat.com/errata/RHSA-2026:59145 https://access.redhat.com/errata/RHSA-2026:59146 https://access.redhat.com/errata/RHSA-2026:59147 https://access.redhat.com/errata/RHSA-2026:59148 https://access.redhat.com/errata/RHSA-2026:59149 https://access.redhat.com/errata/RHSA-2026:59091

Vendor	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-23240, CVE-2026-23449, CVE-2026-31629, CVE-2026-31759, CVE-2026-43077, CVE-2026-43109, CVE-2026-43110, CVE-2026-43206, CVE-2026-46037, CVE-2026-46242, CVE-2026-46274, CVE-2026-46319, CVE-2026-52923, CVE-2026-52956, CVE-2026-52972, CVE-2026-53133, CVE-2026-53182, CVE-2026-53224, CVE-2026-53246, CVE-2026-64530, CVE-2026-64600, CVE-2023-53995, CVE-2026-46331, CVE-2025-40204)
Description	SUSE 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. SUSE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	• openSUSE Leap: 15.4, 15.5, 15.6 • SUSE Linux Enterprise 12 SP5 (High Performance Computing, Live Patching, Server, Server for SAP Applications) • SUSE Linux Enterprise 15 SP4 (High Performance Computing, Live Patching, Real Time, Server, Server for SAP Applications) • SUSE Linux Enterprise 15 SP5 (High Performance Computing, Live Patching, Real Time, Server, Server for SAP Applications) • SUSE Linux Enterprise 15 SP6 (Live Patching, Real Time, Server, Server for SAP Applications) • SUSE Linux Enterprise 15 SP7 (Live Patching, Real Time, Server, Server for SAP Applications) • SUSE Linux Enterprise Micro: 5.3, 5.4, 5.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/

Vendor	**Dell**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-20716, CVE-2026-63693, CVE-2026-27110, CVE-2026-28257, CVE-2026-28258)
Description	Dell 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. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	• Dell PowerEdge R470, R570, R670, R770, XE9780, XE9780L, XE7740: BIOS prior to v1.9.5 • Dell PowerEdge R770AP, XE9780LAP: BIOS prior to v1.7.4 • Dell PowerEdge XR8720t: BIOS prior to v1.3.4 • Dell Inspiron 15 3510: BIOS prior to v1.30.0 • Dell Inspiron 15 3521: BIOS prior to v1.25.0 • Dell XPS 8950: BIOS prior to v1.33.0 • Dell XPS 8960: BIOS prior to v2.24.0 • Dell AppSync: v4.6.0.4, v4.6.1.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000502468/dsa-2026-356-security-update-for-dell-poweredge-server-for-intel-processor-firmware-vulnerability • https://www.dell.com/support/kbdoc/en-us/000501826/dsa-2026-280-security-update-for-dell-client-platform-bios-for-an-improper-link-resolution-before-file-access-link-following-vulnerability • https://www.dell.com/support/kbdoc/en-us/000502484/dsa-2026-165-security-update-for-dell-appsync-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	IBM WebSphere Hybrid Edition: 5.1 IBM WebSphere Application Server Liberty: 17.0.0.3 – 26.0.0.8 IBM WebSphere Application Server: 9.0.0.0 – 9.0.5.28 IBM Cloud Pak for Security: 1.10.0.0 – 1.10.11.0 IBM QRadar Suite Software: 1.10.12.0 – 1.11.10.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7284710 https://www.ibm.com/support/pages/node/7284718 https://www.ibm.com/support/pages/node/7284722 https://www.ibm.com/support/pages/node/7284670

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.