Advisory Alert

Alert Number: AAA20260714 **Date:** July 14, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

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

Description

Vendor	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
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	Dell Storage Resource Manager: • vApp - Versions prior to 6.1.1.0 • Windows/Linux update - Versions prior to 6.1.1.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000488837/dsa-2026-311-dell-storage-resource-manager-srm-and-dell-storage-monitoring-and-reporting-smr-security-update-for-multiple-third-party-component-vulnerabilities

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-39821, CVE-2026-42264, CVE-2026-42044, CVE-2026-42043, CVE-2025-62718, CVE-2026-46595, CVE-2026-42508, CVE-2026-39834, CVE-2026-39833, CVE-2026-39832, CVE-2026-39831, CVE-2026-39830, CVE-2026-4800)
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 Db2 Genius Hub versions 1.1, 1.1.1, 1.1.2 Agentics version 1.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7279901

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-68183, CVE-2026-31408, CVE-2026-43074, CVE-2026-43279, CVE-2026-45984, CVE-2026-46135, CVE-2026-46152, CVE-2026-46189, CVE-2026-46242, CVE-2026-46316, CVE-2026-53359)
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 Enterprise Linux 9.6 Extended Update Support: x86_64, aarch64, ppc64le, s390x • Red Hat Enterprise Linux 9.6 Advanced Update Support: x86_64 • Red Hat Enterprise Linux 9.6 Update Services for SAP Solutions: x86_64, ppc64le • Red Hat Enterprise Linux 9.6 Four Years of Updates: aarch64, s390x • Red Hat Enterprise Linux 9.6 Extended Life Cycle: x86_64, aarch64, ppc64le, s390x • Red Hat CodeReady Linux Builder 9.6 Extended Update Support: x86_64, aarch64, ppc64le, s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:38902

Vendor	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE 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. SUSE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	SUSE Linux Enterprise 12 SP5 (SLES, SLES LTSS, SLES LTSS Extended Security, SLES for SAP, HPC, Live Patching) SUSE Linux Enterprise 15 SP4 (SLES, SLES for SAP, HPC, Live Patching, Real Time) SUSE Linux Enterprise 15 SP5 (SLES, SLES for SAP, HPC, Live Patching, Real Time) SUSE Linux Enterprise 15 SP6 (SLES, SLES for SAP, Live Patching, Real Time) SUSE Linux Enterprise 15 SP7 (SLES, SLES for SAP, Live Patching, Real Time) SUSE Linux Enterprise Micro (Versions 5.3, 5.4, 5.5) openSUSE Leap (Versions 15.4, 15.5, 15.6)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2026/suse-su-20262902-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20262914-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20262910-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20262909-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20262899-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20262894-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20262895-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20262890-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20262889-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20262888-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20262887-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20262868-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20262867-1/

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 Db2 Genius Hub versions 1.1, 1.1.1, 1.1.2 Agentics version 1.0 IBM Security Verify Governance Adapter for CyberArk version 10.0.1 IBM Security QRadar Log Management AQL Plugin versions 1.0.0 through 1.1.6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7279901 https://www.ibm.com/support/pages/node/7279850 https://www.ibm.com/support/pages/node/7279853 https://www.ibm.com/support/pages/node/7279924

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.