Advisory Alert

Alert Number: AAA20260925 **Date:** September 25, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

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

Description

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-16439, CVE-2026-16441)
Description	IBM has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-16439:** In Eclipse OpenJ9 versions up to 0.60, using -Xtrace to trace method arguments can lead to buffer underflow. **CVE-2026-16441:** In Eclipse OpenJ9 versions up to 0.60, when executing class files where a previously concrete superclass method has been recompiled as abstract, execution is incorrectly delegated to an interface default method. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Decision Optimization for Cloud Pak for Data version 5.3.1 before Patch 13
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7289345

Vendor	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-6237, CVE-2024-4741, CVE-2026-22796, CVE-2022-43680, CVE-2023-52425, CVE-2023-52426, CVE-2024-28757, CVE-2025-59375, CVE-2025-60876, CVE-2025-66382, CVE-2026-23855, CVE-2026-25210, CVE-2026-32776, CVE-2026-32777, CVE-2026-32778, CVE-2018-1000500, CVE-2021-42374, CVE-2021-42376, CVE-2021-42378, CVE-2021-42379, CVE-2021-42380, CVE-2021-42381, CVE-2021-42382, CVE-2021-42384, CVE-2021-42385, CVE-2021-42386, CVE-2022-28391, CVE-2022-48174, CVE-2025-46394, CVE-2025-35991, CVE-2026-43499, CVE-2026-43503, CVE-2026-46242, CVE-2026-46331, CVE-2026-1965, CVE-2026-4873, CVE-2026-5545, CVE-2026-6253, CVE-2026-6276, CVE-2026-6429, CVE-2026-4046, CVE-2026-5450, CVE-2026-5928, CVE-2026-34743, CVE-2026-28390, CVE-2026-7383, CVE-2026-9076, CVE-2026-34180, CVE-2026-34182, CVE-2026-42766, CVE-2026-42770, CVE-2026-45445, CVE-2026-45446, CVE-2026-45447, CVE-2026-54874, CVE-2026-63072, CVE-2026-63074, CVE-2026-63076, CVE-2026-75803, CVE-2026-9149, CVE-2026-9150, CVE-2026-25707, CVE-2026-44933, CVE-2026-44941, CVE-2026-44942, CVE-2026-48863, CVE-2026-11822, CVE-2026-11824, CVE-2026-80357, CVE-2026-80359, CVE-2026-80358, CVE-2026-81473, CVE-2026-56792)
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 APEX Cloud Platform for Red Hat OpenShift versions prior to 03.07.00.00 • Dell Boot Optimized Server Storage (BOSS) N-1 Firmware versions prior to 2.2.13.2038 • Dell Rugged Control Center Software versions prior to 5.2.206
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000513079/dsa-2026-425-security-update-for-dell-apex-cloud-platform-for-red-hat-openshift-for-multiple-third-party-component-vulnerabilities

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-39964, CVE-2026-53266, CVE-2026-68121, CVE-2026-74469, CVE-2026-80844, CVE-2026-81000, CVE-2026-15809, CVE-2026-34986, CVE-2026-5260, CVE-2026-11822, CVE-2026-11824, CVE-2026-14164, CVE-2026-16313, CVE-2026-46323)
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	RHEL 10.0 • Extended Update Support (EUS): aarch64, ppc64le, s390x, x86_64 • CodeReady Linux Builder (EUS): aarch64, ppc64le, s390x, x86_64 • 4 Years of Updates / Support: aarch64, ppc64le, s390x, x86_64 RHEL 9.2 • Advanced Update Support (AUS): x86_64 • Update Services for SAP Solutions (E4S): ppc64le, x86_64 • 4 Years of Updates: aarch64, s390x • Extended Life Cycle (ELC): aarch64, ppc64le, s390x, x86_64 RHEL 8.8 • Extended Life Cycle Long Life: x86_64 • Telecommunication Update Service (TUS): x86_64 • Update Services for SAP Solutions (E4S): ppc64le, x86_64 RHEL 8.6 • Extended Life Cycle Long Life: aarch64, ppc64le, s390x, x86_64 • Advanced Update Support (AUS): x86_64 RHEL 8.4 • Extended Life Cycle Long Life: aarch64, ppc64le, s390x, x86_64 • Advanced Update Support (AUS): x86_64 Legacy / Extended Support • RHEL 7: Extended Life Cycle Support (ELS) (ppc64, ppc64le, s390x, x86_64) • RHEL 6: Extended Life Cycle Support Extension (ELS) (i386, s390x, x86_64)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:71687 https://access.redhat.com/errata/RHSA-2026:67856 https://access.redhat.com/errata/RHSA-2026:71649 https://access.redhat.com/errata/RHSA-2026:71599 https://access.redhat.com/errata/RHSA-2026:71601 https://access.redhat.com/errata/RHSA-2026:71594 https://access.redhat.com/errata/RHSA-2026:71592 https://access.redhat.com/errata/RHSA-2026:67837 https://access.redhat.com/errata/RHSA-2026:67935 https://access.redhat.com/errata/RHSA-2026:71565

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	openSUSE Leap 15.5 and 15.6 SUSE Linux Enterprise High Performance Computing 12 SP5 SUSE Linux Enterprise Live Patching 12-SP5, 15-SP6 and 15-SP7 SUSE Linux Enterprise Micro 5.5 SUSE Linux Enterprise Real Time 15 SP6 and 15 SP7 SUSE Linux Enterprise Server 12 SP5, 15 SP6 and 15 SP7 SUSE Linux Enterprise Server for SAP Applications 12 SP5, 15 SP6 and 15 SP7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2026/suse-su-20264347-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20264344-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20264342-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20264340-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20264336-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20264328-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20264320-1/

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 20.04, 22.04, 24.04, 26.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-8818-1 https://ubuntu.com/security/notices/USN-8817-1 https://ubuntu.com/security/notices/USN-8816-1

Vendor	**Hitachi**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	Hitachi 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. Hitachi advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Hitachi Virtual Storage Platform 5100, 5200, 5500, 5600, 5100H, 5200H, 5500H and 5600H
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.hitachi.com/products/it/storage-solutions/sec_info/2026/08.html

Vendor	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-69247, CVE-2026-69248, CVE-2026-69249, CVE-2026-71852, CVE-2026-71870, CVE-2026-72848, CVE-2026-75838, CVE-2026-75509, CVE-2026-45819, CVE-2026-73088, CVE-2026-73089, CVE-2026-41254, CVE-2026-47057, CVE-2026-47063, CVE-2026-47058, CVE-2026-60147, CVE-2026-46968, CVE-2026-47027, CVE-2026-47021, CVE-2026-46917, CVE-2026-47059, CVE-2026-47010, CVE-2026-16243)
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 QRadar App SDK version 1.0.0 to 2.2.6 QRadar AI Assistant version 1.0.0 to 2.2.0 QRadar Log Source Management App version 1.0.0 to 7.0.17 Decision Optimization for Cloud Pak for Data version 5.3.1. before Patch 13
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7289320 https://www.ibm.com/support/pages/node/7289341 https://www.ibm.com/support/pages/node/7289363 https://www.ibm.com/support/pages/node/7289345

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.