Advisory Alert

Alert Number: AAA20260602 **Date:** June 2, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
MariaDB	**Critical**	Security Update
Red Hat	**High**	Multiple Vulnerabilities
Ivanthi	**High**	Privilege Escalation Vulnerability
SUSE	**High**	Multiple Vulnerabilities
MariaDB	**High**	Security Update
IBM	**High, Medium, Low**	Multiple Vulnerabilities
Zyxel Networks	**Medium**	Buffer Overflow Vulnerabilities

Description

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-9319, CVE-2026-8644, CVE-2026-9311, CVE-2026-4800, CVE-2026-29063, CVE-2026-42043, CVE-2026-42044)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their product. These vulnerabilities could be exploited by malicious users to compromise affected systems. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM WebSphere Application Server - Versions 8.5 & 9.0 QRadar Log Source Management App – Versions 1.0.0 – 7.0.14 QRadar AI Assistant – Versions 1.0.0 – 1.5.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7274738 • https://www.ibm.com/support/pages/node/7274740 • https://www.ibm.com/support/pages/node/7274733 • https://www.ibm.com/support/pages/node/7274746 • https://www.ibm.com/support/pages/node/7274750

Vendor	**MariaDB**
Severity	**Critical**
Affected Vulnerability	Security Update (CVE-2026-49261)
Description	MariaDB has released a security update addressing a vulnerability that exists in their product. This vulnerability could be exploited by malicious users to compromise affected systems. MariaDB advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	MariaDB Community Server Versions 11.8.8, 11.4.12, 10.11.18, 10.6.27
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://mariadb.com/docs/server/security/cve/community-server

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-56547, CVE-2025-39766, CVE-2026-23210, CVE-2026-31419, CVE-2026-43163)
Description	Red Hat has released a security update addressing multiple vulnerabilities that exist in the kernel of their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux for x86_64 - Extended Update Support 10.0 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 10.0 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 10.0 ppc64le Red Hat Enterprise Linux for ARM 64 - Extended Update Support 10.0 aarch64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 10.0 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 10.0 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 10.0 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 10.0 aarch64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 10.0 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 10.0 s390x Red Hat Enterprise Linux for Power, little endian - 4 years of support 10.0 ppc64le Red Hat Enterprise Linux for x86_64 - 4 years of updates 10.0 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:22334

Vendor	**Ivanti**
Severity	**High**
Affected Vulnerability	Privilege Escalation Vulnerability (CVE-2026-9614)
Description	Ivanti has released a security update addressing a vulnerability that exists in their products. **CVE-2026-9614:** An Improper Access Control vulnerability in Ivanti Neurons for ITSM (cloud and on-premises) allows a remote authenticated attacker to gain administrative access. Ivanti advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ivanti Neurons for ITSM (On-Premises) – Versions 2025.4 and prior Ivanti Neurons for ITSM (Cloud) – Versions 2026.1 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Neurons-for-ITSM-CVE-2026-9614?language=en_US

Vendor	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-54518, CVE-2026-23243, CVE-2026-23274, CVE-2026-23317, CVE-2026-46300, CVE-2026-46333)
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in the kernel of their product. These vulnerabilities could be exploited by malicious users to compromise affected systems. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.4, 15.5 & 15.6 SUSE Linux Enterprise High Performance Computing 12 SP5 SUSE Linux Enterprise High Performance Computing 15 SP4 SUSE Linux Enterprise High Performance Computing 15 SP5 SUSE Linux Enterprise Live Patching 12-SP5 SUSE Linux Enterprise Live Patching 15-SP4 SUSE Linux Enterprise Live Patching 15-SP5 SUSE Linux Enterprise Live Patching 15-SP6 SUSE Linux Enterprise Live Patching 15-SP7 SUSE Linux Enterprise Micro 5.3, 5.4 & 5.5 SUSE Linux Enterprise Real Time 15 SP4 SUSE Linux Enterprise Real Time 15 SP5 SUSE Linux Enterprise Real Time 15 SP6 SUSE Linux Enterprise Real Time 15 SP7 SUSE Linux Enterprise Server 12 SP5 SUSE Linux Enterprise Server 15 SP4 SUSE Linux Enterprise Server 15 SP5 SUSE Linux Enterprise Server 15 SP6 SUSE Linux Enterprise Server 15 SP7 SUSE Linux Enterprise Server for SAP Applications 12 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP4 SUSE Linux Enterprise Server for SAP Applications 15 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP6 SUSE Linux Enterprise Server for SAP Applications 15 SP7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2026/suse-su-20262181-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20262189-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20262191-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20262199-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20262200-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20262207-1/

Vendor	**MariaDB**
Severity	**High**
Affected Vulnerability	Security Update (CVE-2026-48165, CVE-2026-48163)
Description	MariaDB has released a security update addressing multiple vulnerabilities that exists in their product. These vulnerabilities could be exploited by malicious users to compromise affected systems. MariaDB advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	MariaDB Community Server Versions 11.8.8, 11.4.12, 10.11.18, 10.6.27
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://mariadb.com/docs/server/security/cve/community-server

Vendor	**IBM**
Severity	**High, Medium, Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-15599, CVE-2026-0540, CVE-2026-4923, CVE-2026-4926, CVE-2026-41238, CVE-2026-41239, CVE-2026-41240, CVE-2026-2950, CVE-2025-13465, CVE-2026-33671, CVE-2026-33672, CVE-2025-27789, CVE-2026-40895, CVE-2026-41168, CVE-2026-41312, CVE-2026-41313, CVE-2026-41314, CVE-2026-41425, CVE-2026-42033, CVE-2026-42034, CVE-2026-42035, CVE-2026-42036, CVE-2026-42037, CVE-2026-42038, CVE-2026-42039, CVE-2026-42040, CVE-2026-42041, CVE-2026-42042, CVE-2026-41481, CVE-2026-41205, CVE-2026-44431, CVE-2026-44432, CVE-2026-23943)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	PowerVC – Versions 2.2.1.2, 2.3.0, 2.3.1, 2.3.2 QRadar Log Source Management App – Versions 1.0.0 – 7.0.14 QRadar AI Assistant – Versions 1.0.0 – 1.5.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7274664 • https://www.ibm.com/support/pages/node/7274746 • https://www.ibm.com/support/pages/node/7274750

Vendor	**Zyxel Networks**
Severity	**Medium**
Affected Vulnerability	Buffer Overflow Vulnerabilities (CVE-2026-3870, CVE-2026-3871)
Description	Zyxel has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-3870:** A buffer overflow vulnerability in the UPnP AddPortMapping() command in certain DSL/Ethernet CPE firmware versions could allow an adjacent attacker to trigger a temporary denial-of-service (DoS) condition affecting the UPnP function of the affected device. **CVE-2026-3871:** A buffer overflow vulnerability in the UPnP DeletePortMapping() command in certain 4G LTE/5G NR CPE and DSL/Ethernet CPE firmware versions could allow an adjacent attacker to trigger a temporary DoS condition affecting the UPnP function of the affected device. Zyxel advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	DSL/Ethernet CPE • VMG4005-B50B – Versions 5.13(ABRL.5.4)C0 and earlier 4G LTE/5G NR CPE • NR7101 – Versions 1.00(ABUV.11)C0 and earlier • Nebula LTE3301-PLUS – Versions 1.18(ACCA.6)C0 and earlier' • Nebula NR7101 – Versions 1.16(ACCC.1)C0 and earlier DSL/Ethernet CPE • VMG4005-B50B – Versions 5.13(ABRL.5.4)C0 and earlier
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerabilities-in-the-upnp-function-of-certain-4g-lte-5g-nr-cpe-and-dsl-ethernet-cpe-06-02-2026

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.