Advisory Alert

Alert Number: AAA20260721 **Date:** July 21, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
Zyxel Networks	**High**	OS Command Injection Vulnerability
Red Hat	**High**, **Medium**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-48714, CVE-2025-46295)
Description	IBM has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-48714:** In versions prior to 3.9.7, the missingKeyHandler blocked the literal request-body keys __proto__, constructor, and prototype (added in 3.9.3, see GHSA-5fgg-jcpf-8jjw), but did not reject dotted variants such as "__proto__.polluted". Downstream backends that split the missing-key string on a configured keySeparator (notably i18next-fs-backend ≤ 2.6.5) hand these keys to an unguarded setPath() walker that writes to Object.prototype. Applications that expose missingKeyHandler to untrusted input AND use i18next-fs-backend ≤ 2.6.5 are directly exploitable for remote prototype pollution. Other downstream backends that split the missing-key string the same way may be similarly affected. Depending on the host application, polluted prototype properties may cause crashes, corrupted translation behaviour, configuration poisoning, or bypasses of property-based security checks. **CVE-2025-46295:** Apache Commons Text versions prior to 1.10.0 included interpolation features that could be abused when applications passed untrusted input into the text-substitution API. Because some interpolators could trigger actions like executing commands or accessing external resources, an attacker could potentially achieve remote code execution. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Storage Defender - Resiliency Service - Versions 2.0.0 - 2.1.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7279937

Vendor	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
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	SUSE Linux Enterprise Live Patching 15-SP7 SUSE Linux Enterprise Real Time 15 SP7 SUSE Linux Enterprise Server 15 SP7 SUSE Linux Enterprise Server for SAP Applications 15 SP7 SUSE Real Time Module 15-SP7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2026/suse-su-20263130-1/

Vendor	**Zyxel Networks**
Severity	**High**
Affected Vulnerability	OS Command Injection Vulnerability (CVE-2026-6952)
Description	Zyxel Networks has released a security update addressing a vulnerability that exists in their products. **CVE-2026-6952:** A post-authentication command injection vulnerability in the "LogServer" field of the syslog component in certain firmware versions for DSL/Ethernet CPE, Fiber ONTs, and Wireless Extenders could allow an authenticated attacker with administrator privileges to execute OS commands on an affected device. It is important to note that WAN access is disabled by default on these devices, and this attack can succeed only if user-configured passwords have been compromised. Zyxel Networks advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	DSL/Ethernet CPE Models • DX3300-T0, DX3300-T1, DX3301-T0, EX3300-T0, EX3300-T1, EX3301-T0 — 5.50(ABVY.8)C0 and earlier • DX4510-B0, DX4510-B1 — 5.17(ABYL.10.2)C0 and earlier • DX5401-B1, EX5401-B1 — 5.17(ABYO.7.2)C0 and earlier • EE3301-00 — 5.63(ACMU.3.1)C0 and earlier • EE5301-00 — 5.63(ACLD.3.1)C0 and earlier • EE6510-10 — 5.19(ACJQ.4.2)C0 and earlier • EMG3525-T50B, EMG5523-T50B, VMG3625-T50B, VMG8623-T50B — 5.50(ABPM.9.8)C0 and earlier • EX2210-T0 — 5.50(ACDI.2.5)C0 and earlier • EX3500-T0, EX3501-T0 — 5.44(ACHR.5.1)C0 and earlier • EX3600-T0 — 5.70(ACIF.2.1)C0 and earlier • EX5512-T0 — 5.70(ACEG.5.6)C0 and earlier • EX5601-T0, EX5601-T1 — 5.70(ACDZ.6)C0 and earlier • EX7501-B0 — 5.18(ACHN.3.2)C0 and earlier • EX7710-B0 — 5.18(ACAK.1.7)C0 and earlier • GM4100-B0 — 5.18(ACCL.2.1)C0 and earlier • VMG4005-B50A, VMG4005-B60A — 5.17(ABQA.3.3)C0 and earlier Fiber ONTs Models • AM7510-00, PE3301-00 — 5.63(ACOR/ACMT.x)C0 and earlier • AX7501-B1 — 5.17(ABPC.7.2)C0 and earlier • PE5301-01 — 5.63(ACOJ.3.1)C0 and earlier • PM3100-T0, PM5100-T0, PM5100-T1 — 5.42(ACBF.4.3)C0 and earlier • PM7300-T0 — 5.42(ABYY.4.1)C0 and earlier • PM7500-00 — 5.61(ACKK.1.4)C0 and earlier • PX5301-T0 — 5.44(ACKB.0.7)C0 and earlier Wireless Extender Models • WE3300-00 — 5.70(ACKA.2)C0 and earlier • WX3100-T0 — 5.50(ABVL.5)C0 and earlier • WX5600-T0 — 5.70(ACEB.6)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-post-authentication-command-injection-vulnerability-in-certain-dsl-ethernet-cpe-fiber-onts-and-wireless-extenders-07-21-2026

Vendor	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-43499, CVE-2026-35554)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-43499:** A flaw was found in the Linux kernel. When the kernel's real-time mutex (rtmutex) component performs a specific operation called 'proxy-lock rollback' during futex requeue, it incorrectly handles task pointers. This can lead to a 'Use-After-Free' (UAF) vulnerability, where the system attempts to use memory that has already been released. A local attacker could potentially exploit this to gain elevated privileges or execute unauthorized code. **CVE-2026-35554:** A flaw was found in the Apache Kafka Java producer client. A race condition in the client's buffer pool management can cause messages to be silently delivered to incorrect topics. This occurs when a message batch expires while its network request is still active, leading to premature buffer deallocation and potential reuse by other messages. Consequently, sensitive data may be exposed to unauthorized consumers, and data integrity can be compromised through deserialization failures and processing errors. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux Server - Extended Life Cycle Support Extension 6 x86_64 Red Hat Enterprise Linux Server - Extended Life Cycle Support Extension 6 i386 Red Hat Enterprise Linux Server - Extended Life Cycle Support Extension (for IBM z Systems) 6 s390x JBoss Enterprise Application Platform Text-Only Advisories x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:41920 • https://access.redhat.com/errata/RHSA-2026:42098

Vendor	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-34479, CVE-2025-67030, CVE-2026-6873, CVE-2026-7246, CVE-2026-7666, CVE-2026-8404, CVE-2026-9375, CVE-2026-25645, CVE-2026-35193, CVE-2026-41683, CVE-2026-41690, CVE-2026-42353, CVE-2026-44431, CVE-2026-44432, CVE-2026-45409, CVE-2026-48587)
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 Storage Defender - Resiliency Service - Versions 2.0.0 - 2.1.5 IBM Db2 Versions: • 11.5.0 - 11.5.9 • 12.1.0 - 12.1.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7279458 • https://www.ibm.com/support/pages/node/7279937

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	22.04, 24.04, 26.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://ubuntu.com/security/notices/USN-8569-1 • https://ubuntu.com/security/notices/USN-8570-1 • https://ubuntu.com/security/notices/USN-8568-1 • https://ubuntu.com/security/notices/USN-8567-1 • https://ubuntu.com/security/notices/USN-8566-1

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.