Advisory Alert

Alert Number: AAA20260625 **Date:** June 25, 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	**Critical**	Out-of-bounds Write Vulnerability
SUSE	**High**	Multiple Vulnerabilities
Drupal	**High**, **Medium**, **Low**	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 Networking OS10 - Versions prior to 10.6.1.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000480864/dsa-2026-240-security-update-for-dell-networking-os10-vulnerabilities

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-38476, CVE-2024-45337, CVE-2024-57965, CVE-2025-4517, CVE-2025-7783, CVE-2025-14813, CVE-2025-23048, CVE-2025-30223, CVE-2025-49794, CVE-2025-49796, CVE-2025-62718, CVE-2026-1188, CVE-2026-31789, CVE-2026-39821, CVE-2026-39892, CVE-2026-42043, CVE-2026-42044, CVE-2026-42264)
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	WebSphere Liberty Operator - Versions 1.0.0 - 1.6.1 IBM Storage Defender - Resiliency Service - Versions 2.0.0 - 2.1.4 IBM OS Image for AIX Systems - Version 3.1.3.0 IBM Cloud Pak System Versions: • 2.3.4.0 & 2.3.4.1 • 2.3.4.1 iFix1 • 2.3.5.0 • 2.3.6.0 IBM OS Image for Red Hat Linux Systems Versions: • 4.0.4.0 • 4.0.5.0 • 4.0.6.0 • 4.0.7.0 • 5.0.0.0 • 5.0.1.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7277767 https://www.ibm.com/support/pages/node/7276685 https://www.ibm.com/support/pages/node/7254419 https://www.ibm.com/support/pages/node/7277066 https://www.ibm.com/support/pages/node/7260910 https://www.ibm.com/support/pages/node/7237418 https://www.ibm.com/support/pages/node/7237420

Vendor	**Red Hat**
Severity	**Critical**
Affected Vulnerability	Out-of-bounds Write Vulnerability (CVE-2026-43037)
Description	Red Hat has released security updates addressing a vulnerability that exist in their products. **CVE-2026-43037:** A flaw was found in the Linux kernel's IPv6 tunnel implementation. A remote attacker could exploit this flaw by sending malicious ICMPv6 error messages to cause a stack-based buffer overflow in the kernel's IPv4-over-IPv6 tunnel error handling code. This could result in a kernel crash (denial of service) or potentially allow arbitrary code execution with kernel privileges. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux Server - AUS 9.2 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.2 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 9.2 x86_64 Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.2 ppc64le Red Hat Enterprise Linux for x86_64 - Extended Update Support Extension 8.8 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.8 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.8 x86_64 Red Hat Enterprise Linux for x86_64 10 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 10.2 x86_64 Red Hat Enterprise Linux for Power, little endian 10 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 10.2 ppc64le Red Hat Enterprise Linux for Power, little endian - 4 years of support 10.2 ppc64le Red Hat Enterprise Linux for x86_64 - 4 years of updates 10.2 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 10.2 x86_64 Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 10.2 ppc64le Red Hat Enterprise Linux for x86_64 9 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.8 x86_64 Red Hat Enterprise Linux for Power, little endian 9 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.8 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.8 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.8 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 9.8 x86_64 Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.8 ppc64le Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.6 x86_64 Red Hat Enterprise Linux Server - AUS 9.6 x86_64 Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.6 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.6 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.6 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 9.6 x86_64 Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.6 ppc64le Red Hat Enterprise Linux Server - AUS 9.4 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.4 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 9.4 x86_64 Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.4 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:28750 https://access.redhat.com/errata/RHSA-2026:28748 https://access.redhat.com/errata/RHSA-2026:28742 https://access.redhat.com/errata/RHSA-2026:28741 https://access.redhat.com/errata/RHSA-2026:28740 https://access.redhat.com/errata/RHSA-2026:28738

Vendor	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-23278, CVE-2026-31402, CVE-2026-31504, CVE-2026-31694, CVE-2026-43503, CVE-2026-46323)
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 15.4 & 15.6 SUSE Linux Enterprise High Performance Computing 15 SP4 SUSE Linux Enterprise Live Patching 15-SP4 SUSE Linux Enterprise Micro 5.3 SUSE Linux Enterprise Micro 5.4 SUSE Linux Enterprise Real Time 15 SP4 SUSE Linux Enterprise Server 15 SP4 SUSE Linux Enterprise Server for SAP Applications 15 SP4 SUSE Linux Enterprise Live Patching 15-SP6 SUSE Linux Enterprise Real Time 15 SP6 SUSE Linux Enterprise Server 15 SP6 SUSE Linux Enterprise Server for SAP Applications 15 SP6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2026/suse-su-20262607-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20262608-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20262610-1/

Vendor	**Drupal**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-13244, CVE-2026-13243, CVE-2026-13240, CVE-2026-13239, CVE-2026-13238, CVE-2026-13237, CVE-2026-13236, CVE-2026-13235, CVE-2026-13234, CVE-2026-13233, CVE-2026-13231)
Description	Drupal 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. Drupal advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Tealium iQ Tag Management module - All Versions Salesforce module - Version prior to 5.1.3 WissKI module - Version prior to 4.2.0 admin_feedback module - Version prior to 2.8.0 OpenAI Provider module - Version prior to 1.1.1 & 1.2.0 to 1.2.2 AI Agents module Versions • 1.2.17 & prior • 1.3.0 to 1.3.8 • 1.4.0 to 1.4.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/security

Vendor	**IMB**
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	WebSphere Liberty Operator - Versions 1.0.0 - 1.6.1 IBM WebSphere Application Server - Liberty 17.0.0.3 - 25.0.0.9 IBM Storage Defender - Resiliency Service - Versions 2.0.0 - 2.1.4 IBM OS Image for AIX Systems - Version 3.1.3.0 IBM QRadar DNS Analyzer App - Version 1.0.0 - 2.0.4 IBM Cloud Pak System Versions: • 2.3.4.0 & 2.3.4.1 • 2.3.5.0 • 2.3.5.0 (Power) • 2.3.6.0 • 2.3.4.1 iFix1 • 2.3.3.6 iFix1 • 2.3.3.6 iFix2 IBM OS Image for Red Hat Linux Systems Versions: • 4.0.4.0 • 4.0.5.0 • 4.0.6.0 • 4.0.7.0 • 5.0.0.0 • 5.0.1.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/bulletin/

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.