Advisory Alert

Alert Number: AAA20260424 **Date:** April 24, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
IBM	**High, Medium, Low**	Multiple Vulnerabilities
Drupal	**Medium**	Cross Site Scripting Vulnerability

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released security updates addressing multiple vulnerabilities that exists in the third-party components of their product. These vulnerabilities could be exploited by malicious users to compromise affected systems. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell Storage Resource Manager – Versions prior to 6.1.0.0 Dell Storage Monitoring and Reporting – Versions prior to 6.1.0.0 Dell Storage Resource Manager – Versions prior to 6.1.0.0 Dell VxRail Appliance – Versions 8.0.000 through 8.0.370
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000456382/dsa-2026-196-dell-storage-resource-manager-srm-and-dell-storage-monitoring-and-reporting-smr-security-update-for-multiple-third-party-component-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000456372/dsa-2026-126-security-update-for-dell-vxrail-for-multiple-third-party-component-vulnerabilities

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	CVE-2024-38542, CVE-2025-38234, CVE-2025-39998, CVE-2025-68794, CVE-2025-68818, CVE-2025-71231, CVE-2025-71268, CVE-2025-71269, CVE-2026-23030, CVE-2026-23047, CVE-2026-23103, CVE-2026-23120, CVE-2026-23136, CVE-2026-23140, CVE-2026-23187, CVE-2026-23191, CVE-2026-23193, CVE-2026-23201, CVE-2026-23215, CVE-2026-23216, CVE-2026-23231, CVE-2026-23242, CVE-2026-23243, CVE-2026-23255, CVE-2026-23259, CVE-2026-23268, CVE-2026-23270, CVE-2026-23272, CVE-2026-23274, CVE-2026-23277, CVE-2026-23278, CVE-2026-23281, CVE-2026-23292, CVE-2026-23293, CVE-2026-23317, CVE-2026-23319, CVE-2026-23361, CVE-2026-23379, CVE-2026-23381, CVE-2026-23386, CVE-2026-23398, CVE-2026-23413, CVE-2026-23414, CVE-2026-31788
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in the kernel of their products. These vulnerabilities could be exploited by malicious users to compromise 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 SUSE Linux Enterprise High Performance Computing 15 SP5 SUSE Linux Enterprise Live Patching 15-SP5 SUSE Linux Enterprise Live Patching 15-SP7 SUSE Linux Enterprise Micro 5.2 SUSE Linux Enterprise Micro 5.5 SUSE Linux Enterprise Micro for Rancher 5.2 SUSE Linux Enterprise Real Time 15 SP5 SUSE Linux Enterprise Real Time 15 SP7 SUSE Linux Enterprise Server 15 SP5 SUSE Linux Enterprise Server 15 SP7 SUSE Linux Enterprise Server for SAP Applications 15 SP5 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-20261560-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20261573-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20261574-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20261575-1/

Affected Product	**IBM**
Severity	**High, Medium, Low**
Affected Vulnerability	CVE-2025-14831, CVE-2025-9820, CVE-2025-61662, CVE-2026-3497, CVE-2026-2447, CVE-2026-4519, CVE-2025-15281, CVE-2026-0915, CVE-2026-22695, CVE-2026-22801, CVE-2026-25646, CVE-2025-10158, CVE-2025-0938, CVE-2024-26984, CVE-2025-71238, CVE-2026-23193, CVE-2026-23231
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 affected systems. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	QRadar – Versions 7.5.0 - 7.5.0 UP15 IF01
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7270594

Affected Product	**Drupal**
Severity	**Medium**
Affected Vulnerability	Cross Site Scripting Vulnerability (CVE-2026-6871)
Description	Drupal has released a security update addressing a vulnerability that exists in a module of their product. **CVE-2026-6871:** A Cross-Site Scripting (XSS) vulnerability found in the Obfuscate module, where it affects sites using the ROT13 encoding and where an attacker can enter content that is filtered using the module's Twig filter. Drupal advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Obfuscate Module – Versions prior to 2.0.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-contrib-2026-033

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.