Advisory Alert

Alert Number: **AAA20251023** **Date:** **October 23, 2025**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
SUSE	**High**	Multiple Linux Kernel Vulnerabilities
Dell	**High, Medium**	Multiple Vulnerabilities
SolarWinds	**Medium**	SQL Injection Vulnerability

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-38796, CVE-2024-28956, CVE-2024-45332, CVE-2024-48012, CVE-2025-26466, CVE-2024-45490, CVE-2024-45491, CVE-2024-45492, CVE-2024-50602, CVE-2024-2961, CVE-2023-6780, CVE-2024-52533, CVE-2023-52340, CVE-2024-42154)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• Avamar Data Store Gen5A Dell PowerEdge Server BIOS - Versions prior to 2.24.0 • Avamar Data Store Gen5A Integrated Dell Remote Access Controller (iDRAC) - Versions prior to 7.00.00.181
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000362542/dsa-2025-339-security-update-for-dell-avamar-data-store-gen5a-multiple-third-party-component-vulnerabilities

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Linux Kernel Vulnerabilities
Description	SUSE has released security updates addressing multiple linux kernel vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	OpenSUSE Leap 15.4, 15.5 SUSE Real Time Module 15-SP7 SUSE Linux Enterprise Micro 5.3, 5.4, 5.5 SUSE Linux Enterprise Micro for Rancher 5.3, 5.4 SUSE Linux Enterprise Server 15 SP4, 15 SP5, 15 SP7 SUSE Linux Enterprise Real Time 15 SP4, 15 SP5, 15 SP7 SUSE Linux Enterprise Live Patching 15-SP4, 15-SP5, 15-SP7 SUSE Linux Enterprise High Performance Computing 15 SP4, 15 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP4, 15 SP5, 15 SP7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2025/suse-su-20253712-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20253716-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20253717-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20253720-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20253721-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20253725-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20253731-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20253734-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20253733-1/

Affected Product	**Dell**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-20052, CVE-2025-20101, CVE-2025-20018, CVE-2025-20003, CVE-2025-21099, CVE-2025-20041, CVE-2025-20071, CVE-2025-20031, CVE-2024-45371, CVE-2024-47800, CVE-2024-46895, CVE-2024-28954, CVE-2024-29222, CVE-2024-39758, CVE-2024-31150)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000281808/dsa-2025-078

Affected Product	**SolarWinds**
Severity	**Medium**
Affected Vulnerability	SQL Injection Vulnerability (CVE-2025-26392)
Description	SolarWinds has released security updates addressing a sql injection vulnerability that exists in their products. **CVE-2025-26392 -** SolarWinds Observability Self-Hosted is susceptible to SQL injection vulnerability that may display sensitive data using a low-level account. This vulnerability requires authentication from a low-privilege account. SolarWinds advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SolarWinds Observability Self-Hosted 2025.2.1 and prior versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.solarwinds.com/trust-center/security-advisories/cve-2025-26392

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.