Advisory Alert

Alert Number: AAA20250214 **Date:** February 14, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
PostgreSQL	**High**	SQL Injection Vulnerability
SUSE	**High**	Multiple Vulnerabilities
Dell	**High**, Medium	Multiple Vulnerabilities
cPanel	Medium	Multiple Vulnerabilities

Description

Affected Product	**PostgreSQL**
Severity	**High**
Affected Vulnerability	SQL Injection Vulnerability (CVE-2025-1094)
Description	PostgreSQL has released security updates addressing an SQL Injection vulnerability that exists in some PostgreSQL functions. **CVE-2025-1094** - Improper neutralization of quoting syntax in PostgreSQL libpq functions PQescapeLiteral(), PQescapeIdentifier(), PQescapeString(), and PQescapeStringConn() allows a database input provider to achieve SQL injection in certain usage patterns. Specifically, SQL injection requires the application to use the function result to construct input to psql, the PostgreSQL interactive terminal. Similarly, improper neutralization of quoting syntax in PostgreSQL command line utility programs allows a source of command line arguments to achieve SQL injection when client_encoding is BIG5 and server_encoding is one of EUC_TW or MULE_INTERNAL. PostgreSQL advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PostgreSQL versions before 17.3, 16.7, 15.11, 14.16, and 13.19
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.postgresql.org/about/news/postgresql-173-167-1511-1416-and-1319-released-3015/

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-4244, CVE-2023-52923, CVE-2024-35863, CVE-2024-50199, CVE-2024-53104, CVE-2024-56600, CVE-2024-56601, CVE-2024-56623, CVE-2024-56650, CVE-2024-56658, CVE-2024-56664, CVE-2024-56759, CVE-2024-57791, CVE-2024-57798, CVE-2024-57849, CVE-2024-57893)
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 system. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.3 SUSE Enterprise Storage 7.1 SUSE Linux Enterprise High Availability Extension 15 SP3 SUSE Linux Enterprise High Performance Computing 15 SP3 SUSE Linux Enterprise High Performance Computing LTSS 15 SP3 SUSE Linux Enterprise Live Patching 15-SP3 SUSE Linux Enterprise Micro 5.1 SUSE Linux Enterprise Micro 5.2 SUSE Linux Enterprise Micro for Rancher 5.2 SUSE Linux Enterprise Server 15 SP3 SUSE Linux Enterprise Server 15 SP3 Business Critical Linux SUSE Linux Enterprise Server 15 SP3 LTSS SUSE Linux Enterprise Server for SAP Applications 15 SP3 SUSE Manager Proxy 4.2 SUSE Manager Retail Branch Server 4.2 SUSE Manager Server 4.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2025/suse-su-20250517-1/

Affected Product	**Dell**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-22480, CVE-2025-23380)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in Dell SupportAssist OS Recovery and Dell PowerEdge BIOS. **CVE-2025-22480** - Dell SupportAssist OS Recovery versions prior to 5.5.13.1 contain a symbolic link attack vulnerability. A low-privileged attacker with local access could potentially exploit this vulnerability, leading to arbitrary file deletion and Elevation of Privileges. **CVE-2025-23380** - Dell PowerEdge RAID Controller S160, version(s) 7.3.0.3, contain(s) an Improper Input Validation vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Unauthorized access. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• Dell SupportAssist OS Recovery Software versions prior to 5.5.13.1 • BIOS versions prior to 1.10.6 of Dell XC Core XC7625 • BIOS versions prior to 2.3.5 of PowerEdge R660, PowerEdge R760, PowerEdge C6620, PowerEdge MX760c, PowerEdge R860, PowerEdge R960, PowerEdge HS5610, PowerEdge HS5620, PowerEdge R660xs, PowerEdge R760xs, PowerEdge R760xd2, PowerEdge T560, PowerEdge R760xa, PowerEdge XE9680, PowerEdge XR5610, PowerEdge XR8610t, PowerEdge XR8620t, PowerEdge XR7620, PowerEdge XE8640, PowerEdge XE9640, Dell XC Core XC660, Dell XC Core XC760, Dell XC Core XC660xs, Dell XC Core XC760xa • BIOS versions prior to 1.4.3 of PowerEdge T160, PowerEdge R260, PowerEdge T360, PowerEdge R360, PowerEdge C6615 • BIOS versions prior to 1.9.5 of PowerEdge R6615, PowerEdge R7615, PowerEdge R6625, PowerEdge R7625 • BIOS versions prior to 1.15.2 of PowerEdge R650, PowerEdge R750, PowerEdge R750XA, PowerEdge C6520, PowerEdge MX750C, PowerEdge R550, PowerEdge R450, PowerEdge R650XS, PowerEdge R750XS, PowerEdge T550, PowerEdge XR11, PowerEdge XR12, Dell EMC XC Core XC450, Dell EMC XC Core XC650, Dell EMC XC Core XC750, Dell EMC XC Core XC750xa, Dell EMC XC Core XC6520 • BIOS versions prior to 1.16.2 of PowerEdge XR4510c and PowerEdge XR4520c • BIOS versions prior to 1.10.2 of PowerEdge T150, PowerEdge T350, PowerEdge R250, PowerEdge R350 • BIOS versions prior to 2.16.1 of PowerEdge R6515 and PowerEdge R7515 • BIOS versions prior to 2.16.3 of PowerEdge R6525, PowerEdge R7525 and Dell EMC XC Core XC7525 • BIOS versions prior to 2.16.2 of PowerEdge C6525 • BIOS versions prior to 2.15.2 of PowerEdge XE8545
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000275712/dsa-2025-051 • https://www.dell.com/support/kbdoc/en-us/000284712/dsa-2025-066-security-update-for-dell-poweredge-raid-controller-s160-vulnerability

Affected Product	**cPanel**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-0167, CVE-2025-0665, CVE-2025-0725, CVE-2024-56337, CVE-2025-23419)
Description	cPanel 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. cPanel advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	All versions of libcurl through 8.11.1 All versions of Tomcat 10.1 through 10.1.34 All versions of NGINX through 1.26.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://news.cpanel.com/easyapache4-v25-5-maintenance-and-security-release/

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.