Advisory Alert

Alert Number: AAA20250509 **Date:** May 9, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Red Hat	**Medium**	Time-of-Check to Time-of-Use Vulnerability
PostgreSQL	**Medium**	Buffer Over-read Vulnerability

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-24980, CVE-2024-24853, CVE-2023-22351, CVE-2024-21871, CVE-2023-25546, CVE-2023-42772, CVE-2024-21829, CVE-2024-21781, CVE-2023-41833, CVE-2023-43753, CVE-2024-23984, CVE-2024-24968, CVE-2024-21853, CVE-2024-38303, CVE-2024-38304, CVE-2024-21820, CVE-2024-23918, CVE-2024-25565, CVE-2024-36242, CVE-2024-24985, CVE-2024-22185, CVE-2024-21944, CVE-2024-27457, CVE-2024-21925, CVE-2024-21924, CVE-2024-21936, CVE-2024-21935, CVE-2024-21927, CVE-2023-20508, CVE-2023-20582, CVE-2023-20581, CVE-2023-31345, CVE-2024-56161, CVE-2024-38796, CVE-2024-36347, CVE-2023-52340, CVE-2024-42154, CVE-2024-52046, CVE-2024-24852, CVE-2024-36274, CVE-2024-6387, CVE-2024-20286, CVE-2024-20285, CVE-2024-20284, CVE-2024-20289, CVE-2024-20413, CVE-2024-20411, CVE-2024-20397, CVE-2025-22224, CVE-2025-22225, CVE-2025-22226)
Description	Dell has released security update addressing multiple vulnerabilities that exist in Dell PowerFlex Rack 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	PowerFlex rack RCM - Versions prior to 3.7.7.0 PowerFlex rack RCM - Versions prior to 3.8.2.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000318891/dsa-2025-204-security-update-for-dell-powerflex-rack-multiple-third-party-component-vulnerabilities

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Time-of-Check to Time-of-Use Vulnerability (CVE-2024-56337)
Description	Red Hat has released a security update addressing a Time-of-Check to Time-of-Use Vulnerability in their products. **CVE-2024-56337 -** The fix for CVE-2024-50379 in Apache Tomcat was insufficient to mitigate the issue fully. A Time-of-check Time-of-use (TOCTOU) race condition occurs during JSP compilation on case-insensitive file systems when the default servlet is enabled for writing. This vulnerability allows an uploaded file to be treated as a JSP and executed, resulting in remote code execution. Red Hat advises applying the security fixes as soon as possible to protect systems from potential threats.
Affected Products	JBoss Enterprise Web Server 5 for RHEL 9 x86_64 JBoss Enterprise Web Server 5 for RHEL 8 x86_64 JBoss Enterprise Web Server 5 for RHEL 7 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2025:4521

Affected Product	**PostgreSQL**
Severity	**Medium**
Affected Vulnerability	Buffer Over-read Vulnerability (CVE-2025-4207)
Description	PostgreSQL has released a security update addressing a Buffer Over-read Vulnerability in their products. **CVE-2025-4207 -** A buffer over-read in PostgreSQL GB18030 encoding validation allows a database input provider to achieve temporary denial of service on platforms where a 1-byte over-read can elicit process termination. This affects the database server and also libpq. PostgreSQL advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PostgreSQL Versions before 17.5, 16.9, 15.13, 14.18, and 13.21
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.postgresql.org/support/security/CVE-2025-4207/

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.