Advisory Alert

Alert Number: AAA20251029 **Date:** October 29, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
IBM	**Critical**	SQL injection Vulnerability
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Red Hat	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-40242, CVE-2022-26872, CVE-2022-2827)
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 products. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PowerSwitch Z9264F-ON Firmware - Versions prior to 3.42.5.1-21
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000384884/dsa-2025-408-security-update-for-dell-networking-products-for-multiple-vulnerabilities

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	SQL injection Vulnerability (CVE-2025-59681)
Description	IBM has released security updates addressing a SQL injection vulnerability that exist in their products. **CVE-2025-59681 -** An issue was discovered in Django 4.2 before 4.2.25, 5.1 before 5.1.13, and 5.2 before 5.2.7. QuerySet.annotate(), QuerySet.alias(), QuerySet.aggregate(), and QuerySet.extra() are subject to SQL injection in column aliases, when using a suitably crafted dictionary, with dictionary expansion, as the **kwargs passed to these methods (on MySQL and MariaDB). IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Storage Defender - Resiliency Service - Versions 2.0.0 - 2.0.17
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7248617

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-32988, CVE-2025-32989, CVE-2025-32990, CVE-2025-58754, CVE-2025-4673, CVE-2025-8916, CVE-2025-59682)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause denial of service, confidential information exposure, out-of-bound write. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Storage Defender - Resiliency Service - Versions 2.0.0 - 2.0.17
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7248617

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-50070, CVE-2022-50137, CVE-2022-50228, CVE-2023-53125, CVE-2023-53305, CVE-2025-22026, CVE-2025-37797, CVE-2025-38556, CVE-2025-39730, CVE-2025-39751, CVE-2025-38718, CVE-2025-39682)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause buffer overflow, use-after-free, userspace injects. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.2 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.2 s390x Red Hat Enterprise Linux Server - AUS 8.6 x86_64, AUS 9.2 x86_64, TUS 8.6 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.6 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.2 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support Extension 8.6 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.6 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:19222 • https://access.redhat.com/errata/RHSA-2025:19224

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.