



Advisory Alert

Alert Number: AAA20250805 Date: August 5, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Red Hat	High, Medium	Multiple Vulnerabilities
Dell	Medium	Multiple Vulnerabilities

Description

Affected Product	Red Hat
Severity	High, Medium
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-21727, CVE-2025-21928, CVE-2025-21929, CVE-2025-22020, CVE-2025-22085, CVE-2025-22113, CVE-2025-37890, CVE-2025-38052, CVE-2025-38086, CVE-2025-38087, CVE-2025-38264, CVE-2022-49788, CVE-2025-21962, CVE-2022-50020, CVE-2025-38079, CVE-2022-49995, CVE-2024-57980, CVE-2025-21905, CVE-2025-23150, CVE-2025-37958, CVE-2022-49058, CVE-2022-50022, CVE-2025-22004, CVE-2025-37738)
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 use-after-free, integer overflow, double free and buffer overflow. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.6 ppc64le - Red Hat Enterprise Linux Server - AUS 9.6 x86_64. AUS 8.2 x86_64 - Red Hat Enterprise Linux for x86_64 9 x86_64, 10 x86_64 - Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.6 x86_64, 9.0 x86_64 - Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.6 x86_64, 10.0 x86_64 - Red Hat Enterprise Linux for x86_64 - 4 years of updates 10.0 x86_64 - Red Hat Enterprise Linux for Real Time for NFV 8 x86_64 - Red Hat Enterprise Linux for Real Time 8 x86_64 - Red Hat Enterprise Linux for Power, little endian 9 ppc64le, 10 ppc64le - Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.6, 10.0 ppc64le - Red Hat Enterprise Linux for Power, little endian - 4 years of support 10.0 ppc64le - Red Hat Enterprise Linux for IBM z Systems 9 s390x, 10 s390x - Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.6 s390x, 10.0 s390x - Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.6 s390x, 10.0 s390x - Red Hat Enterprise Linux for ARM 64 9 aarch64, 10 aarch64 - Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.6 aarch64, 10.0 aarch64 - Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.6 aarch64, 10.0 aarch64 - Red Hat CodeReady Linux Builder for x86_64 9 x86_64, 10 x86_64 - Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.6 x, 10.0 x86_64 - Red Hat CodeReady Linux Builder for Power, little endian 9 ppc64le, 10 ppc64le - Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.6 ppc64le, 10.0 ppc64le - Red Hat CodeReady Linux Builder for IBM z Systems 9 s390x, 10 s390x - Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.6, 10.0 s390x - Red Hat CodeReady Linux Builder for ARM 64 9 aarch64, 10 aarch64 - Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.6, 10.0 aarch64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2025:12662 https://access.redhat.com/errata/RHSA-2025:12746 https://access.redhat.com/errata/RHSA-2025:12753 https://access.redhat.com/errata/RHSA-2025:12525 https://access.redhat.com/errata/RHSA-2025:12623

Affected Product	Dell
Severity	Medium
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-28956, CVE-2024-45332, CVE-2025-20103, CVE-2025-20054, CVE-2025-21464, CVE-2025-2884)
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	Precision 7920 Rack BIOS Versions prior to 2.24.0 Precision 7920 XL Rack BIOS Versions prior to 2.24.0 Precision 7960 Rack BIOS Versions prior to 2.6.3 Precision 7960 XL Rack BIOS Versions prior to 2.6.3 Inspiron 14 5441 BIOS Versions prior to 2.10.1 Inspiron 14 7441 BIOS Versions prior to 2.10.1 Latitude 5455 BIOS Versions prior to 2.10.1 Latitude 7455 BIOS Versions prior to 2.10.1 XPS 13 9345 BIOS Versions prior to 2.8.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000317403/dsa-2025-199 https://www.dell.com/support/kbdoc/en-us/000294892/dsa-2025-127

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.