



Advisory Alert

Alert Number: AAA20250912 Date: September 12, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	Critical	Multiple Vulnerabilities
SUSE	High	Multiple Vulnerabilities
Red Hat	High	Multiple Vulnerabilities

Description

Affected Product	Dell
Severity	Critical
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released security updates addressing multiple vulnerabilities that exist in third party products which affect Dell PowerProtect Data Protection Hardware. 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	Versions prior to 2.7.9 of PowerProtect Data Protection Firmware <ul style="list-style-type: none">PowerProtect DP Series-IDPA 2.7.9 Upgrade for DP4400 and DP5900 AppliancesPowerProtect DP Series-IDPA 2.7.9 Upgrade for DP8xxx Appliances
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000368282/dsa-2025-300-security-update-for-dell-powerprotect-dp-series-appliance-idpa-multiple-third-party-component-vulnerabilities

Affected Product	SUSE
Severity	High
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-49053, CVE-2024-47674, CVE-2024-47706, CVE-2024-49867, CVE-2025-21999, CVE-2025-37890, CVE-2025-38000, CVE-2025-38001, CVE-2025-38212)
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 15.4 SUSE Linux Enterprise High Performance Computing 15 SP4 SUSE Linux Enterprise Live Patching 15-SP4 SUSE Linux Enterprise Micro 5.3, 5.4 SUSE Linux Enterprise Real Time 15 SP4 SUSE Linux Enterprise Server 15 SP4 SUSE Linux Enterprise Server for SAP Applications 15 SP4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	<ul style="list-style-type: none">https://www.suse.com/support/update/announcement/2025/suse-su-202503180-1/https://www.suse.com/support/update/announcement/2025/suse-su-202503179-1/https://www.suse.com/support/update/announcement/2025/suse-su-202503165-1/https://www.suse.com/support/update/announcement/2025/suse-su-202503175-1/https://www.suse.com/support/update/announcement/2025/suse-su-202503160-1/https://www.suse.com/support/update/announcement/2025/suse-su-202503156-1/

Affected Product	Red Hat
Severity	High
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-2513, CVE-2024-42094, CVE-2024-50102, CVE-2025-22058, CVE-2025-22097, CVE-2025-37914, CVE-2025-38079, CVE-2025-38085, CVE-2025-38159, CVE-2025-38211, CVE-2025-38250, CVE-2025-38332, CVE-2025-38352, CVE-2025-38464)
Description	<p>Red Hat 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.</p> <p>Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.</p>
Affected Products	<p>Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.4 aarch64</p> <p>Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.4 s390x</p> <p>Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.4 ppc64le</p> <p>Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.4 x86_64</p> <p>Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.0 aarch64</p> <p>Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.2 aarch64</p> <p>Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.4 aarch64</p> <p>Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.4 aarch64</p> <p>Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.0 s390x</p> <p>Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.2 s390x</p> <p>Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.4 s390x</p> <p>Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.4 s390x</p> <p>Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.4 ppc64le</p> <p>Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.4 x86_64</p> <p>Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.0 x86_64</p> <p>Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.2 x86_64</p> <p>Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.4 x86_64</p> <p>Red Hat Enterprise Linux Server - AUS 9.2 x86_64</p> <p>Red Hat Enterprise Linux Server - AUS 9.2 x86_64 AUS 9.4 x86_64</p> <p>Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.0 ppc64le</p> <p>Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le</p> <p>Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le</p>
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	<ul style="list-style-type: none">https://access.redhat.com/errata/RHSA-2025:15670https://access.redhat.com/errata/RHSA-2025:15669https://access.redhat.com/errata/RHSA-2025:15668

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.