Advisory Alert

| Alert Number: | AAA20250812 | Date: | August 12, 2025 |

Document Classification Level	**:**	Public Circulation Permitted | Public
Information Classification Level	**:**	TLP: WHITE

Overview

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

Description

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-26466, CVE-2024-45490, CVE-2024-50602, CVE-2024-2961, CVE-2024-52533, CVE-2023-6780, CVE-2024-4741, CVE-2024-6119, CVE-2024-9143, CVE-2024-45762, CVE-2024-38796, CVE-2024-28956, CVE-2024-36293, CVE-2024-39279, CVE-2024-28047, CVE-2025-31651, CVE-2025-31650, CVE-2025-22235, CVE-2025-27820)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in Dell PowerProtect Data Manager Appliance (DM5500). 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	PowerProtect DM5500 - PowerProtect Data Manager Appliance (DM5500), dmas-upgrade-5.19.1.0-196.pkg - Versions prior to 5.19.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000355635/dsa-2025-301-security-update-for-dell-powerprotect-data-manager-appliance-dm5500-for-multiple-vulnerabilities

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-47670, CVE-2024-56644, CVE-2025-21727, CVE-2025-21759, CVE-2025-38085, CVE-2025-38159, CVE-2025-38079, CVE-2025-38292)
Description	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. 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 Red Hat Enterprise Linux for x86_64 9 x86_64, 8 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.6 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.6 x86_64 Red Hat Enterprise Linux for Power, little endian 9 ppc64le, 8 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.6 ppc64le Red Hat Enterprise Linux for IBM z Systems 9 s390x, 8 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.6 s390x Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.6 s390x Red Hat Enterprise Linux for ARM 64 9 aarch64, 8 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.6 aarch64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.6 aarch64 Red Hat CodeReady Linux Builder for x86_64 9 x86_64, 8 x86_64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.6 x86_64 Red Hat CodeReady Linux Builder for Power, little endian 9 ppc64le, 8 ppc64le Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.6 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems 9 s390x Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.6 s390x Red Hat CodeReady Linux Builder for ARM 64 9 aarch64, 8 aarch64 Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.6 aarch64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:13589 • https://access.redhat.com/errata/RHSA-2025:13602

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.

Financial Sector Computer Security Incident Response Team (FinCSIRT)
LankaPay Pvt Ltd, 'The Zenith', 161A, Dharmapala Mawatha, Colombo 07, Sri Lanka
Hotline: + 94 112039777

Public Circulation Permitted \| Public   Report incidents to incident@fincsirt.lk   TLP: WHITE