# Advisory Alert

**Alert Number:** AAA20260623 **Date:** June 23, 2026

**Document Classification Level :** Public Circulation Permitted | Public

**Information Classification Level :** TLP: WHITE

## Overview

| Vendor | Severity | Vulnerability |
|---|---|---|
| **Red Hat** | **High** | Multiple Vulnerabilities |
| **Dell** | **High** | Multiple Vulnerabilities |

## Description

| | |
|---|---|
| Vendor | **Red Hat** |
| Severity | **High** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2026-28780, CVE-2026-49975, CVE-2026-34032, CVE-2026-34059, CVE-2026-33007, CVE-2026-33857, CVE-2026-29169, CVE-2026-29168, CVE-2025-53020, CVE-2026-27135, CVE-2026-2673, CVE-2026-45186, CVE-2026-31790, CVE-2026-31474, CVE-2026-31669, CVE-2026-31787, CVE-2026-31772, CVE-2026-43260, CVE-2026-43279, CVE-2026-43414, CVE-2026-46331, CVE-2026-45984, CVE-2026-46056, CVE-2026-46152, CVE-2026-46117, CVE-2026-46145, CVE-2026-46125, CVE-2026-46173, CVE-2026-46166, CVE-2026-46135) |
| 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 systems.<br>Red Hat advises to apply these security fixes at your earliest to protect your systems from potential threats. |
| Affected Products | • Red Hat JBoss Core Services 1 for RHEL 8 and 7 x86_64<br>• Red Hat JBoss Core Services Text-Only Advisories x86_64<br>• Red Hat Enterprise Linux for x86_64 9 x86_64<br>• Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.8 x86_64<br>• Red Hat Enterprise Linux for IBM z Systems 9 s390x<br>• Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.8 s390x<br>• Red Hat Enterprise Linux for Power, little endian 9 ppc64le<br>• Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.8 ppc64le<br>• Red Hat Enterprise Linux for ARM 64 9 aarch64<br>• Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.8 aarch64<br>• Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.8 ppc64le<br>• Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.8 x86_64<br>• Red Hat CodeReady Linux Builder for x86_64 9 x86_64<br>• Red Hat CodeReady Linux Builder for Power, little endian 9 ppc64le<br>• Red Hat CodeReady Linux Builder for ARM 64 9 aarch64<br>• Red Hat CodeReady Linux Builder for IBM z Systems 9 s390x<br>• Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.8 x86_64<br>• Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.8 ppc64le<br>• Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.8 s390x<br>• Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.8 aarch64<br>• Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.8 aarch64<br>• Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.8 s390x<br>• Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 9.8 x86_64<br>• Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 9.8 aarch64<br>• Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.8 ppc64le<br>• Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 9.8 s390x |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | • https://access.redhat.com/errata/RHSA-2026:27200<br>• https://access.redhat.com/errata/RHSA-2026:27201<br>• https://access.redhat.com/errata/RHSA-2026:27789 |

| | |
|---|---|
| Vendor | **Dell** |
| Severity | **High** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2025-3360, CVE-2025-4373, CVE-2025-40909, CVE-2025-24528, CVE-2025-6297) |
| Description | Dell has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems.<br>Dell advises to apply these security fixes at your earliest to protect your systems from potential threats. |
| Affected Products | Dell PowerProtect Data Manager Appliance DM5510 version 6.22.0.0 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | • https://www.dell.com/support/kbdoc/en-us/000480323/dsa-2026-260-security-update-for-dell-powerprotect-data-manager-appliance-dm5510-multiple-vulnerabilities |

## 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.