# Advisory Alert

**Alert Number:** AAA20241002 **Date:** October 2, 2024

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

**Information Classification Level :** TLP: WHITE

## Overview

| Product | Severity | Vulnerability |
|---|---|---|
| **Dell** | **Critical** | Multiple Vulnerabilities |
| **Dell** | **High** | Multiple Vulnerabilities |
| **Red hat** | **Medium** | Multiple Vulnerabilities |
| **F5** | **Low** | Heap-based Buffer Overflow Vulnerability |

## Description

| | |
|---|---|
| Affected Product | **Dell** |
| Severity | **Critical** |
| Affected Vulnerability | Multiple Vulnerabilities |
| 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.<br>Dell advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | Multiple Products |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | • https://www.dell.com/support/kbdoc/en-us/000227304/dsa-2024-314-security-update-for-dell-powerprotect-dd-idrac9-vulnerabilities<br>• https://www.dell.com/support/kbdoc/en-us/000228411/dsa-2024-387-security-update-for-multiple-dell-thinos-vulnerabilities<br>• https://www.dell.com/support/kbdoc/en-us/000226833/dsa-2024-311-security-update-for-dell-vxflex-ready-node-and-powerflex-custom-node-multiple-third-party-component-vulnerabilities |

| | |
|---|---|
| Affected Product | **Dell** |
| Severity | **High** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2024-6387, CVE-2024-20284, CVE-2024-20285, CVE-2024-20286, CVE-2024-21147, CVE-2024-21145, CVE-2024-21140, CVE-2024-21144, CVE-2024-21131, CVE-2024-21138, CVE-2022-41946) |
| Description | Dell has released security updates addressing multiple vulnerabilities that exist in third party products which affect Dell products. These vulnerabilities could be exploited by malicious users to compromise the affected system.<br>Dell advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | Dell Protection Advisor Versions 19.8,19.9 and 19.10<br>NX-OS Versions prior to 9.4 (2) running on:<br>Connectrix MDS-9124V, Connectrix MDS-9148V, Connectrix MDS-9396V, Connectrix MDS-9706-V2, Connectrix MDS-9710-V2, Connectrix MDS-9718-V3, Connectrix MDS-9132T, Connectrix MDS-9148T, Connectrix MDS-9396T, Connectrix MDS-9220i, Connectrix MDS-9148S, Connectrix MDS-9250i, Connectrix MDS-9396S, Connectrix MDS-9706, Connectrix MDS-9710, Connectrix MDS-9718<br>**DD OS Versions 7.7.1 through 8.1.0.0** running on: Dell PowerProtect DD series appliances, Dell PowerProtect DD Virtual Edition, Dell APEX Protection Storage, Dell PowerProtect DD Management Center, Dell PowerProtect DD Management Center with SmartScale feature, Data Domain Operating System (DD OS), Dell PowerProtect DD appliance models: DD3300, DD6400, DD6900, DD9400, DD9900<br>**DD OS Versions 8.0.0.0 through 8.1.0.0** running on: Dell PowerProtect DD appliance models: DD9410, DD9910<br>**DD OS 7.13 Versions prior to 7.13.1.05** running on: Dell PowerProtect DD series appliances, Dell PowerProtect DD Virtual Edition, Dell APEX Protection Storage, Dell PowerProtect DD Management Center, Dell PowerProtect DD Management Center with SmartScale feature, Dell PowerProtect DD appliance models: DD3300, DD6400, DD6900, DD9400, and DD9900, Data Domain Operating System (DD OS) LTS2024 7.13.1<br>**DD OS 7.10 Versions prior to 7.10.1.40** running on: Dell PowerProtect DD series appliances, Dell PowerProtect DD Virtual Edition, Dell APEX Protection Storage, Dell PowerProtect DD Management Center, Dell PowerProtect DD Management Center with SmartScale feature, Dell PowerProtect DD appliance models: DD3300, DD6400, DD6900, DD9400, and DD9900, Data Domain Operating System (DD OS) LTS2023 7.10.1<br>**DD OS 7.7 Versions prior to 7.7.5.50** running on: Dell PowerProtect DD series appliances, Dell PowerProtect DD Virtual Edition, Dell APEX Protection Storage, Dell PowerProtect DD Management Center, Dell PowerProtect DD appliance models: DD3300, DD6400, DD6900, DD9400, and DD9900, Data Domain Operating System (DD OS) LTS2022 7.7.5<br>**PowerProtect Data Protection Software Versions prior to 2.7.7** running on: PowerProtect DP Series Appliance - IDPA (Integrated Data Protection Appliance): All Models, Data Domain Operating System, DD OS 7.10.1.40 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | • https://www.dell.com/support/kbdoc/en-us/000227030/dsa-2024-330-security-update-for-dell-powerprotect-dd-openssh-vulnerability<br>• https://www.dell.com/support/kbdoc/en-us/000231067/dsa-2024-402-security-update-for-dell-connectrix-mds-cisco-multiple-third-party-component-vulnerabilities<br>• https://www.dell.com/support/kbdoc/en-us/000230941/dsa-2024-411-security-update-for-data-protection-advisor-for-multiple-vulnerabilities |

| | |
|---|---|
| Affected Product | **Red Hat** |
| Severity | **Medium** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2024-26923, CVE-2024-36270, CVE-2024-27415, CVE-2024-36979, CVE-2024-38558) |
| 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.<br>Red Hat advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | Red Hat Enterprise Linux Server - AUS 8.6 x86_64<br>Red Hat Enterprise Linux Server - AUS 9.2 x86_64<br>Red Hat Enterprise Linux Server - TUS 8.6 x86_64<br>Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.6 ppc64le<br>Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.6 x86_64<br>Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.2 x86_64<br>Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.2 s390x<br>Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.2 ppc64le<br>Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.2 aarch64<br>Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le<br>Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.2 x86_64<br>Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.2 x86_64<br>Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.2 ppc64le<br>Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.2 s390x<br>Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.2 aarch64<br>Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.2 aarch64<br>Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.2 s390x<br>Red Hat Enterprise Linux for Real Time for x86_64 - 4 years of updates 9.2 x86_64<br>Red Hat Enterprise Linux for Real Time for NFV for x86_64 - 4 years of updates 9.2 x86_64 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | • https://access.redhat.com/errata/RHSA-2024:7486<br>• https://access.redhat.com/errata/RHSA-2024:7489<br>• https://access.redhat.com/errata/RHSA-2024:7490 |

| | |
|---|---|
| Affected Product | **F5** |
| Severity | **Low** |
| Affected Vulnerability | Heap-based Buffer Overflow Vulnerability (CVE-2018-6913) |
| Description | F5 has released security updates addressing a Heap-based Buffer Overflow Vulnerability that exists in third party product Perl which affects F5 products.<br>**CVE-2018-6913** - Heap-based buffer overflow in the pack function in Perl before 5.26.2 allows context-dependent attackers to execute arbitrary code via a large item count.<br>F5 advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | BIG-IP versions:<br>17.1.0 - 17.1.1<br>16.1.0 - 16.1.5<br>15.1.0 - 15.1.10<br>BIG-IQ Centralized Management versions 8.2.0 - 8.3.0 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://my.f5.com/manage/s/article/K000141301 |

**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.**