# Advisory Alert

**Alert Number:** AAA20240731 **Date:** July 31, 2024

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

**Information Classification Level :** TLP: WHITE

## Overview

| Product | Severity | Vulnerability |
|---|---|---|
| **Dell** | **Critical** | Multiple Vulnerabilities |
| **HPE** | **Critical** | Multiple Vulnerabilities |
| **Dell** | **High** | Multiple Vulnerabilities |
| **Red Hat** | **Medium** | 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 that in turn affect Dell Power Protect Data Manager. 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 Power Protect Data Manager Versions prior to 19.17 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.dell.com/support/kbdoc/en-us/000227331/dsa-2024-334-security-update-dell-power-protect-data-manager-for-multiple-security-vulnerabilities |

| | |
|---|---|
| Affected Product | **HPE** |
| Severity | **Critical** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2024-3596, CVE-2024-41915, CVE-2024-41916, CVE-2024-5486) |
| Description | HPE has released security updates addressing multiple vulnerabilities that exist in their products.<br>**CVE-2024-3596** - A forgery attack has been discovered against the Response Authenticator in RADIUS/UDP, specifically targeting RFC 2865. This attack allows a man-in-the-middle to forge a valid Access-Accept response to a client request that was initially rejected by the RADIUS server, thereby granting unauthorized network access.<br>**CVE-2024-41915** - A vulnerability in the web-based management interface of ClearPass Policy Manager could allow an authenticated remote attacker to conduct SQL injection attacks against the ClearPass Policy Manager instance.<br>**CVE-2024-41916/ CVE-2024-5486** - A vulnerability exists in ClearPass Policy Manager that allows for an attacker with administrative privileges to access sensitive information in a cleartext format.<br>HPE advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | HPE ClearPass Policy Manager 6.12.x: 6.12.1 and below<br>HPE ClearPass Policy Manager 6.11.x: 6.11.8 and below |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04675en_us&docLocale=en_US |

| | |
|---|---|
| Affected Product | **Dell** |
| Severity | **High** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2023-38709, CVE-2023-50387, CVE-2024-2004, CVE-2022-48622, CVE-2024-4453, CVE-2021-47146, CVE-2021-47162, CVE-2021-47188, CVE-2022-48636, CVE-2022-48650, CVE-2022-48688, CVE-2022-48695, CVE-2022-48701, CVE-2023-2860, CVE-2023-52646, CVE-2023-52650, CVE-2023-52652, CVE-2023-52653, CVE-2024-26929, CVE-2024-26930, CVE-2024-26931, CVE-2024-26948, CVE-2024-26993, CVE-2024-27013, CVE-2024-27014, CVE-2024-27043, CVE-2024-27046, CVE-2024-27054, CVE-2024-27072, CVE-2024-27073, CVE-2024-27074, CVE-2024-27075, CVE-2024-27078, CVE-2024-27388, CVE-2024-26458, CVE-2024-26461, CVE-2024-25629, CVE-2018-11490, CVE-2024-31744, CVE-2024-28182, CVE-2024-0727, CVE-2024-4317, CVE-2024-0450, CVE-2022-25236, CVE-2023-52425, CVE-2017-9271, CVE-2023-51764, CVE-2023-42465, CVE-2023-22655, CVE-2023-28746, CVE-2023-38575, CVE-2023-39368, CVE-2023-43490, CVE-2023-45733, CVE-2023-45745, CVE-2023-46103) |
| Description | Dell has released security updates addressing multiple vulnerabilities that exist in third-party products that in turn affect Dell Cyber Sense. 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 Cyber Sense Version 8.6 and prior |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.dell.com/support/kbdoc/en-us/000227418/dsa-2024-338-security-update-for-dell-cyber-sense-for-multiple-third-party-vulnerabilities |

| | |
|---|---|
| Affected Product | **Red Hat** |
| Severity | **Medium** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2021-47459, CVE-2022-48743, CVE-2023-52458, CVE-2023-52809, CVE-2024-26737, CVE-2024-26773, CVE-2024-26852, CVE-2024-26880, CVE-2024-26982, CVE-2024-27030, CVE-2024-27046, CVE-2024-35857, CVE-2024-35885, CVE-2024-35907, CVE-2024-36924, CVE-2024-36952, CVE-2024-38580) |
| Description | Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Null pointer dereferences, Denial of service, Use-after-free conditions, Race conditions.<br>Red Hat advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | Red Hat Enterprise Linux for x86_64 9 x86_64<br>Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.4 x86_64<br>Red Hat Enterprise Linux Server - AUS 9.4 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 9.4 s390x<br>Red Hat Enterprise Linux for Power, little endian 9 ppc64le<br>Red Hat Enterprise Linux for Real Time 9 x86_64<br>Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.4 ppc64le<br>Red Hat Enterprise Linux for Real Time for NFV 9 x86_64<br>Red Hat Enterprise Linux for ARM 64 9 aarch64<br>Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.4 aarch64<br>Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le<br>Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.4 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 9.4 x86_64<br>Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.4 ppc64le<br>Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.4 s390x<br>Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.4 aarch64<br>Red Hat Enterprise Linux Server for ARM 64 - 4 years of updates 9.4 aarch64<br>Red Hat Enterprise Linux Server for IBM z Systems - 4 years of updates 9.4 s390x<br>Red Hat Enterprise Linux for Real Time for x86_64 - 4 years of updates 9.4 x86_64<br>Red Hat Enterprise Linux for Real Time for NFV for x86_64 - 4 years of updates 9.4 x86_64 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://access.redhat.com/errata/RHSA-2024:4928 |

**Disclaimer**

**The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.**