Advisory Alert

Alert Number: AAA20240320 **Date:** March 20, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
Ubuntu	**High**, Medium	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released security updates addressing Multiple Vulnerabilities in their products. Exploitation of these vulnerabilities could lead to Null pointer dereference, Use-after-free, Denial of service, Unauthorized access. Dell recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Dell EMC VxRail Appliance Versions prior to 7.0.483 Dell PowerProtect DD Management Center - Versions 7.0 through 7.12 Dell PowerProtect DD Management Center LTS2023 7.10 - Versions 7.10.1.0 through 7.10.1.15 Dell PowerProtect DD Management Center LTS2022 7.7 - Versions 7.7.5.0 through 7.7.5.25 Dell PowerProtect DD Management Center with SmartScale feature - Versions 7.8 through 7.12 Dell PowerProtect DD Management Center with SmartScale feature LTS2023 7.10 - Versions 7.10.1.0 through 7.10.1.20
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000223302/dsa-2024-144-dell-technologies-powerprotect-dd-management-center-security-update-for-multiple-security-vulnerabilities https://www.dell.com/support/kbdoc/en-us/000223304/dsa-2024-145-dell-technologies-powerprotect-dd-management-center-with-smartscale-feature-security-update-for-multiple-security-vulnerabilities https://www.dell.com/support/kbdoc/en-us/000223311/dsa-2024-049-dell-vxrail-security-update-for-multiple-third-party-component-vulnerabilities-7-0-483

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-0646, CVE-2022-45869, CVE-2023-6606, CVE-2023-2176, CVE-2022-38096, CVE-2023-5633, CVE-2023-6932, CVE-2023-6817, CVE-2023-28772, CVE-2023-31436, CVE-2023-4921, CVE-2023-31084, CVE-2023-7192, CVE-2023-30456, CVE-2023-33952, CVE-2022-36402, CVE-2022-38457, CVE-2023-2166, CVE-2022-41858, CVE-2023-51042, CVE-2023-40283, CVE-2023-4459, CVE-2023-3611, CVE-2022-28388, CVE-2023-1382, CVE-2022-3545, CVE-2023-45862, CVE-2024-1086, CVE-2023-6610, CVE-2024-0565, CVE-2023-6931, CVE-2023-33951, CVE-2022-3594, CVE-2021-43975, CVE-2022-4744, CVE-2023-51043, CVE-2022-40133, CVE-2022-45887)
Description	Red Hat has released a security update addressing Multiple Vulnerabilities in their products. This could lead to Null pointer dereference, Use-after-free, Out-of-bounds write, Slab-out-of-bound read. Red Hat recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.4 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.4 x86_64 Red Hat Enterprise Linux for Real Time - Telecommunications Update Service 8.4 x86_64 Red Hat Enterprise Linux for Real Time for NFV - Telecommunications Update Service 8.4 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.8 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 8.8 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.8 ppc64le Red Hat Enterprise Linux Server - TUS 8.8 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 8.8 aarch64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.8 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.8 x86_64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 8.8 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 8.8 ppc64le Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 8.8 aarch64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2024:1377 https://access.redhat.com/errata/RHSA-2024:1382 https://access.redhat.com/errata/RHSA-2024:1404

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2015-1782, CVE-2020-16135, CVE-2021-33631, CVE-2021-3634, CVE-2021-3696, CVE-2023-1667, CVE-2023-2283, CVE-2023-37536, CVE-2023-46838, CVE-2023-47233, CVE-2023-51042, CVE-2023-51043, CVE-2023-51385, CVE-2023-51780, CVE-2023-51782, CVE-2023-5388, CVE-2023-6004, CVE-2023-6040, CVE-2023-6356, CVE-2023-6535, CVE-2023-6536, CVE-2023-6918, CVE-2023-7207, CVE-2024-0340, CVE-2024-0775, CVE-2024-1086, CVE-2024-20918, CVE-2024-20919, CVE-2024-20921, CVE-2024-20926, CVE-2024-20945, CVE-2024-20952, CVE-2024-21626, CVE-2024-25062)
Description	Dell has released a security update addressing Multiple Vulnerabilities in their products. these Vulnerabilities could be exploited by malicious users to compromise the affected system. Dell recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Data Protection Central OS Update (SUSE SLES 12 SP5) - Version 19.5 through 19.10.0-4 with Data Protection Central OS Update prior to dpc-osupdate-1.1.17-1 Data Protection Central OS Update for Power Protect DP Series Appliances - Version 2.7.6 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000223264/dsa-2024-127-security-update-for-dell-data-protection-central-for-third-party-component-vulnerabilities

Affected Product	**Ubuntu**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-23004, CVE-2024-24855, CVE-2023-23000, CVE-2024-1086)
Description	Ubuntu has released a security update addressing multiple vulnerabilities that exist in their Linux kernel. An attacker may exploit these vulnerabilities to cause Denial of service and Arbitrary code execution. Ubuntu recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Ubuntu 20.04 Ubuntu 18.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-6702-1

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.