Advisory Alert

Alert Number: AAA20240807 **Date:** August 7, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Commvault	**Critical**	SQL Injection Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
SUSE	**High**	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 products. 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	• Dell XtremIO X2 , XMS Versions prior to 6.4.2-13 • Dell Protection Advisor Versions 19.7,19.8 and 19.9 • Dell Avamar Server Hardware Appliance Gen4T/ Gen5A Versions 19.4, 19.7, 19.8, 19.9, 19.10, 19.10-SP1 running SUSE Linux Enterprise 12 SP5 • Dell Avamar Virtual Edition Versions 19.4, 19.7, 19.8, 19.9, 19.10, 19.10-SP1 running SUSE Linux Enterprise 12 SP5 (including Azure and AWS deployments) • Dell Avamar NDMP Accelerator Versions 19.4, 19.7, 19.8, 19.9, 19.10, 19.10-SP1 running SUSE Linux Enterprise 12 SP5 • Dell Avamar VMware Image Proxy Versions 19.4, 19.7, 19.8, 19.9, 19.10, 19.10-SP1 running SUSE Linux Enterprise 12 SP5 • Dell Networker Virtual Edition (NVE) Versions 19.4.x, 19.5.x, 19.6.x, 19.7.x, 19.8.x, 19.9.x, 19.10.x, 19.11.x running SUSE Linux Enterprise 12 SP5 • Dell Power Protect DP Series Appliance / Dell Integrated Data Protection Appliance (IDPA)Version 2.7.x running on SLES12SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000227569/dsa-2024-008-security-update-for-dell-xtremio-x2-multiple-component-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000227571/dsa-2024-347-security-update-for-data-protection-advisor-for-multiple-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000227573/dsa-2024-348-security-update-for-dell-avamar-dell-networker-virtual-edition-nve-and-dell-powerprotect-dp-series-appliance-dell-integrated-data-protection-appliance-idpa-security-update-for-multiple-vulnerabilities

Affected Product	**Commvault**
Severity	**Critical**
Affected Vulnerability	SQL Injection Vulnerability
Description	Commvault has released security updates addressing an SQL injection vulnerability that exists in Commvault command line scripts on all supported versions of the thier software. Commvault advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Commvault software Feature Release 11.34, 11.32, 11.28, 11.24, 11.20
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://documentation.commvault.com/securityadvisories/CV_2024_08_1.html

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-47393, CVE-2022-48637, CVE-2023-52458, CVE-2023-52486, CVE-2023-52635, CVE-2023-52809, CVE-2023-52885, CVE-2024-26601, CVE-2024-26640, CVE-2024-26737, CVE-2024-26810, CVE-2024-26826, CVE-2024-26870, CVE-2024-26930, CVE-2024-26947, CVE-2024-26961, CVE-2024-27030, CVE-2024-27062, CVE-2024-33621, CVE-2024-35789, CVE-2024-35823, CVE-2024-35885, CVE-2024-35896, CVE-2024-35962, CVE-2024-36000, CVE-2024-36017, CVE-2024-36020, CVE-2024-36489, CVE-2024-36929, CVE-2024-36960, CVE-2024-38384, CVE-2024-38555, CVE-2024-38663)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Use After Free Condition, Denial of service, NULL Pointer Dereference. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.2 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.2 s390x Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.2 ppc64le Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.2 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.2 aarch64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.2 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.2 ppc64le Red Hat Enterprise Linux for Real Time for NFV for x86_64 - 4 years of updates 9.2 x86_64 Red Hat Enterprise Linux for Real Time for x86_64 - 4 years of updates 9.2 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.2 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.6 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.2 x86_64 Red Hat Enterprise Linux Server - AUS 8.6 x86_64 Red Hat Enterprise Linux Server - AUS 9.2 x86_64 Red Hat Enterprise Linux Server - TUS 8.6 x86_64 Red Hat Enterprise Linux Server for ARM 64 - 4 years of updates 9.2 aarch64 Red Hat Enterprise Linux Server for IBM z Systems - 4 years of updates 9.2 s390x Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.6 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2024:5065 • https://access.redhat.com/errata/RHSA-2024:5066 • https://access.redhat.com/errata/RHSA-2024:5067

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-47383, CVE-2023-1829, CVE-2024-26828, CVE-2024-26923, CVE-2024-27398, CVE-2024-35950, CVE-2021-46955, CVE-2022-48651, CVE-2024-23307, CVE-2024-26610, CVE-2024-26852)
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Use after free conditions, Memory corruption, Integer Overflow or Wraparound, out-of-bounds read. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.3 SUSE Linux Enterprise High Performance Computing 15 SP2, 15 SP3 SUSE Linux Enterprise Live Patching 15-SP2, 15-SP3 SUSE Linux Enterprise Micro 5.1, 5.2 SUSE Linux Enterprise Server 15 SP2 ,15 SP3 SUSE Linux Enterprise Server for SAP Applications 15 SP2 , 15 SP3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2024/suse-su-20242771-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20242773-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20242792-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20242793-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20242797-1/

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.