Advisory Alert

Alert Number: AAA20240401 **Date:** April 1, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Suse	**High**	Multiple Vulnerabilities
NETGEAR	**High**	Multiple Vulnerabilities
Dell	**High**, Medium	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2017-11164, CVE-2017-7244, CVE-2017-7246, CVE-2020-14155, CVE-2023-26159, CVE-2023-48795, CVE-2023-5941, CVE-2024-25952, CVE-2024-25953, CVE-2024-25954, CVE-2024-25959, CVE-2024-25960, CVE-2024-25961, CVE-2024-25963)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in Dell PowerScale products. These vulnerabilities could be exploited by malicious users to compromise the affected system. Dell recommends to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell PowerScale OneFS - Version 8.2.2 through 9.3.0.0 Dell PowerScale OneFS - Version 9.4.0.0 through 9.7.0.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000223366/dsa-2024-115-security-update-for-dell-powerscale-onefs-for-multiple-security-vulnerabilities

Affected Product	**Suse**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-51779, CVE-2023-6531, CVE-2023-51779, CVE-2023-39191, CVE-2023-46813, CVE-2023-0461)
Description	Suse has released a security update for Linux Kernel. Exploitation of these vulnerabilities could lead to Use-after-free condition, Arbitrary code execution, Escalation of privileges. Suse recommends to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	OpenSUSE Leap 15.3, 15.5, 15.4 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 SUSE Linux Enterprise High Performance Computing 12 SP5 SUSE Linux Enterprise Live Patching 12-SP5 SUSE Linux Enterprise Server 12 SP5 SUSE Linux Enterprise Server for SAP Applications 12 SP5 SUSE Linux Enterprise High Performance Computing 15 SP5 SUSE Linux Enterprise Live Patching 15-SP5 SUSE Linux Enterprise Micro 5.5 SUSE Linux Enterprise Real Time 15 SP5 SUSE Linux Enterprise Server 15 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP5 SUSE Linux Enterprise High Performance Computing 15 SP4 SUSE Linux Enterprise Live Patching 15-SP4 SUSE Linux Enterprise Micro 5.3, 5.4 SUSE Linux Enterprise Real Time 15 SP4 SUSE Linux Enterprise Server 15 SP4 SUSE Linux Enterprise Server for SAP Applications 15 SP4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2024/suse-su-20241017-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20241025-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20241023-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20241039-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20241028-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20241033-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20241047-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20241045-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20241040-1 • https://www.suse.com/support/update/announcement/2024/suse-ru-20241055-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20241054-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20241053-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20241063-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20241072-1

Affected Product	**NETGEAR**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	NETGEAR has released security updates addressing multiple vulnerabilities that exist in their Modems, Wi-Fi Systems and Routers. Exploitation of these vulnerabilities could lead to post-authentication stack overflow, Post-Authentication Command Injection. NETGEAR recommends to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	CBR750 fixed in firmware version 4.6.14.4 C6300v2 fixed in firmware version 1.3.13 RBK852 fixed in firmware version 4.6.7.13 RBR850 fixed in firmware version 4.6.7.13 RBS850 fixed in firmware version 4.6.7.13 R7000 fixed in firmware version 1.0.11.216
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://kb.netgear.com/000066083/Security-Advisory-for-Post-Authentication-Command-Injection-on-R7000-PSV-2024-0013 • https://kb.netgear.com/000066085/Security-Advisory-for-Post-Authentication-Stack-Overflow-on-R7000-PSV-2023-0147 • https://kb.netgear.com/000066086/Security-Advisory-for-Security-Misconfiguration-on-Some-Modems-and-WiFi-Systems-PSV-2021-0131

Affected Product	**Dell**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released a security update addressing Multiple Vulnerabilities. Exploitation of these vulnerabilities could lead to Path Traversal, Sensitive Data Disclosure and system compromise. Dell recommends to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Unisphere for PowerMax - Versions prior to 9.2.4.9 Unisphere for PowerMax Virtual Appliance - Versions prior to 9.2.4.9 Unisphere for PowerMax - Versions prior to 10.0.1.10 Unisphere for PowerMax - Versions prior to 10.1.0.5 Unisphere 360 - Versions prior to 9.2.4.16 Solutions Enabler - Versions prior to 9.2.4.6 Solutions Enabler - Versions prior to 10.0.1.6 Solutions Enabler - Versions prior to 10.1.0.1 Solutions Enabler Virtual Appliance - Versions prior to 9.2.4.6 Dell PowerMax EEM - Version 5978 Dell PowerMax EEM - Version 10.0.1.5 Dell PowerMax EEM - Version 10.1.0.2 PowerMaxOS 5978.714.714 - Version 5978.714.714 PowerMaxOS 10.0.1.5 - Version 10.0.1.5 PowerMaxOS 10.1.0.2 - Version 10.1.0.2 Dell OpenManage Enterprise - 4.0 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000223609/dsa-2024-108-dell-powermaxos-5978-dell-powermax-os-10-0-1-5-dell-powermax-os-10-1-0-2-dell-unisphere-360-unisphere-powermax-unisphere-powermax-vapp-dell-solutions-enabler-vapp-and-dell-powermax-eem-security-update-for-multiple-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000223623/dsa-2024-100-security-update-for-dell-openmanage-enterprise-path-traversal-sensitive-data-disclosure-vulnerability

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.