Advisory Alert

Alert Number: AAA20241210 **Date:** December 10, 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
IBM	**High**, Medium	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-37143, CVE-2024-37144)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2024-37143** - Dell PowerFlex appliance versions prior to IC 46.381.00 and IC 46.376.00, Dell PowerFlex rack versions prior to RCM 3.8.1.0 (for RCM 3.8.x train) and prior to RCM 3.7.6.0 (for RCM 3.7.x train), Dell PowerFlex custom node using PowerFlex Manager versions prior to 4.6.1.0, Dell InsightIQ versions prior to 5.1.1, and Dell Data Lakehouse versions prior to 1.2.0.0 contain an Improper Link Resolution Before File Access vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability to execute arbitrary code on the system. **CVE-2024-37144** - Dell PowerFlex appliance versions prior to IC 46.381.00 and IC 46.376.00, Dell PowerFlex rack versions prior to RCM 3.8.1.0 (for RCM 3.8.x train) and prior to RCM 3.7.6.0 (for RCM 3.7.x train), Dell PowerFlex custom node using PowerFlex Manager versions prior to 4.6.1.0, Dell InsightIQ versions prior to 5.1.1, and Dell Data Lakehouse versions prior to 1.2.0.0 contain an Insecure Storage of Sensitive Information vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to information disclosure. The attacker may be able to use information disclosed to gain unauthorized access to pods within the cluster. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell PowerFlex appliance - Intelligent Catalog (IC) - Versions prior to 46.381.00 Dell PowerFlex rack - Release Certification Matrix (RCM) - Versions prior to 3.8.1.0 Dell PowerFlex custom node - PowerFlex Manager - Versions prior to 4.6.1.0 Dell InsightIQ - Installation Package - Versions prior to 5.1.1 Dell Data Lakehouse - Bundle - Versions prior to 1.2.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000258342/dsa-2024-405-security-update-for-dell-products-for-multiple-vulnerabilities

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-35949, CVE-2024-43861, CVE-2021-47598, CVE-2024-40954, CVE-2024-41059, CVE-2021-46955, CVE-2021-47291, CVE-2021-47378, CVE-2021-47383, CVE-2021-47402, CVE-2021-47600, CVE-2022-48651, CVE-2023-1829, CVE-2023-52752, CVE-2024-23307, CVE-2024-26828, CVE-2024-26852, CVE-2024-26923, CVE-2024-27398, CVE-2024-35861, CVE-2024-35862, CVE-2024-35864, CVE-2024-35950, CVE-2024-36904, CVE-2024-36964, CVE-2024-26610, CVE-2022-48662, CVE-2023-52502, CVE-2023-52846, CVE-2023-6546, CVE-2024-26766, CVE-2024-26930, CVE-2024-35817, CVE-2024-35863, CVE-2024-35867, CVE-2024-35905, CVE-2024-36899)
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to memory leakage, use-after-free conditions, integer overflow, memory corruption, script injection, cross-site scripting. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.3, 15.4 SUSE Linux Enterprise High Performance Computing 12 SP5, 15 SP2, 15 SP3, 15 SP4 SUSE Linux Enterprise Live Patching 12-SP5 SUSE Linux Enterprise Live Patching 15-SP2 SUSE Linux Enterprise Live Patching 15-SP3 SUSE Linux Enterprise Live Patching 15-SP4 SUSE Linux Enterprise Micro 5.1, 5.2, 5.3, 5.4 SUSE Linux Enterprise Real Time 15 SP4 SUSE Linux Enterprise Server 12 SP5, 15 SP2, 15 SP3, 15 SP4 SUSE Linux Enterprise Server for SAP Applications 12 SP5, 15 SP2, 15 SP3, 15 SP4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2024/suse-su-20244261-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20244262-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20244263-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20244264-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20244265-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20244266-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20244268-1/

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-39249, CVE-2024-5569, CVE-2020-11022, CVE-2019-11358, CVE-2020-11023, CVE-2020-23064, CVE-2024-45296)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause denial of service, credential harvesting. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Storage Scale 5.1.9.0 - 5.1.9.6 IBM Storage Scale 5.2.0.0 - 5.2.1.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7178266

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.