Advisory Alert

Alert Number: AAA20221122 **Date:** November 22, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
Ubuntu	**Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-23089, CVE-2022-23091, CVE-2022-33934, CVE-2022-34438, CVE-2022-34439, CVE-2022-34444, CVE-2022-34445, CVE-2022-34454)
Description	Dell has released a security update to address multiple vulnerabilities that exist in their Dell PowerScale oneFs product. Exploitation of these vulnerabilities could cause denial of service, Information disclosure, storing malicious HTML or JavaScript code through multiple affected fields, full system compromise, data leakage, and system takeover. Dell recommends to apply the necessary patch updates at your earliest to avoid issues
Affected Products	Dell PowerScale OneFS versions 8.2.x, 9.0.0.x, 9.1.0.x, 9.2.0.x, 9.2.1.x, 9.3.0.x, and 9.4.0.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000205618/dsa-2022-271

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities(CVE-2022-2601, CVE-2022-3775,CVE-2022-44638, CVE-2021-20206, CVE-2022-42898, CVE-2020-10749 , CVE-2021-37750)
Description	SUSE has released security updates addressing multiple vulnerabilities that exists in their products and packages. Successful exploitation of the most severe vulnerabilities could cause buffer overflow, integer underflow, heap out of bounds write, and arbitrary path write. SUSE recommends to apply the necessary updates at your earliest to avoid issues
Affected Products	openSUSE Leap 15.3, 15.4 openSUSE Leap Micro 5.2, 5.3 SUSE CaaS Platform 4.0 SUSE Enterprise Storage 6, 7, 7.1 SUSE Linux Enterprise Desktop 15-SP3, 15-SP4 SUSE Linux Enterprise High Performance Computing 15, 15-ESPOS, 15-LTSS, 15-SP1-ESPOS, 15-SP1-LTSS, 15-SP2-ESPOS, 15-SP2-LTSS, 15-SP3, 15-SP4 SUSE Linux Enterprise Micro 5.1, 5.2, 5.3 SUSE Linux Enterprise Module for Basesystem 15-SP3 SUSE Linux Enterprise Module for Basesystem 15-SP4 SUSE Linux Enterprise Module for Desktop Applications 15-SP3 SUSE Linux Enterprise Module for Packagehub Subpackages 15-SP3 SUSE Linux Enterprise Module for Public Cloud 15 SUSE Linux Enterprise Module for Server Applications 15-SP4 SUSE Linux Enterprise Module for SUSE Manager Proxy 4.3 SUSE Linux Enterprise Server 12-SP2-BCL, 12-SP3-BCL SUSE Linux Enterprise Server 15, 15-LTSS, 15-SP1-BCL, 15-SP1-LTSS, 15-SP2-BCL, 15-SP2-LTSS, 15-SP3, 15-SP4 SUSE Linux Enterprise Server for SAP 15, 15-SP1, 15-SP2 SUSE Linux Enterprise Server for SAP Applications 15, 15-SP3, 15-SP4 SUSE Manager Proxy 4.1, 4.2, 4.3 SUSE Manager Retail Branch Server 4.1, 4.2, 4.3 SUSE Manager Server 4.1, 4.2, 4.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2022/suse-su-20224140-1/ https://www.suse.com/support/update/announcement/2022/suse-su-20224141-1/ https://www.suse.com/support/update/announcement/2022/suse-su-20224142-1/ https://www.suse.com/support/update/announcement/2022/suse-su-20224143-1/ https://www.suse.com/support/update/announcement/2022/suse-su-20224144-1/ https://www.suse.com/support/update/announcement/2022/suse-su-20224148-1/ https://www.suse.com/support/update/announcement/2022/suse-su-20224150-1/ https://www.suse.com/support/update/announcement/2022/suse-su-20224151-1/ https://www.suse.com/support/update/announcement/2022/suse-su-20224153-1/ https://www.suse.com/support/update/announcement/2022/suse-su-20224154-1/ https://www.suse.com/support/update/announcement/2022/suse-su-20224155-1/

Affected Product	**Ubuntu**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-39253, CVE-2022-39260, CVE-2017-6888, CVE-2020-0499, CVE-2021-0561)
Description	Ubuntu has released a security update to address multiple vulnerabilities that exist in the packages that used in their products. Exploitation of these vulnerabilities could cause denial of service, sensitive information disclosure, arbitrary code execution and cause unexpected behavior in the system. Ubuntu recommends to apply the necessary patch updates at your earliest to avoid issues
Affected Products	Ubuntu 22.10 – GIT versions before git - 1:2.37.2-1ubuntu1.1 Ubuntu 22.04 – FLAC package versions before flac - 1.3.3-2ubuntu0.1, libflac++6v5 - 1.3.3-2ubuntu0.1, libflac8 - 1.3.3-2ubuntu0.1 Ubuntu 20.04 – FLAC package versions before flac - 1.3.3-1ubuntu0.1,libflac++6v5 - 1.3.3-1ubuntu0.1, libflac8 - 1.3.3-1ubuntu0.1 Ubuntu 18.04 - FLAC package versions before flac - 1.3.2-1ubuntu0.1, libflac++6v5 - 1.3.2-1ubuntu0.1, libflac8 - 1.3.2-1ubuntu0.1 Ubuntu 16.04 – FLAC package versions before flac - 1.3.1-4ubuntu0.1~esm1, libflac++6v5 - 1.3.1-4ubuntu0.1~esm1, libflac8 - 1.3.1-4ubuntu0.1~esm1 Ubuntu 14.04 - flac - 1.3.0-2ubuntu0.14.04.1+esm1, libflac++6 - 1.3.0-2ubuntu0.14.04.1+esm1 libflac8 - 1.3.0-2ubuntu0.14.04.1+esm1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-5733-1 https://ubuntu.com/security/notices/USN-5686-3

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.