Advisory Alert

Alert Number: AAA20230317 **Date:** March 17, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Suse	**High**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**Suse**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-4203, CVE-2022-38096, CVE-2022-4129, CVE-2023-0597, CVE-2023-1118, CVE-2023-23559, CVE-2023-26545, CVE-2022-3523, CVE-2023-0461, CVE-2023-22995, CVE-2023-22998, CVE-2023-23000, CVE-2023-23004, CVE-2023-25012, CVE-2022-38096, CVE-2022-4129, CVE-2023-0597, CVE-2023-1118, CVE-2023-23559, CVE-2021-4203, CVE-2022-2991, CVE-2022-36280, CVE-2023-0045, CVE-2023-0590, CVE-2023-22995, CVE-2023-23000, CVE-2023-23006, CVE-2022-3606, CVE-2022-47929, CVE-2023-0179, CVE-2023-0266, CVE-2023-1076, CVE-2023-1095, CVE-2023-1195, CVE-2023-22998, CVE-2023-23004, CVE-2023-25012)
Description	Suse has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities could lead to integer overflow, use-After-Free condition, out-of-bounds memory access, heap-based overflow. Suse recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	openSUSE Leap 15.4 openSUSE Leap Micro 5.3 SUSE CaaS Platform 4.0 SUSE Enterprise Storage 7, 7.1 SUSE Linux Enterprise High Availability Extension 12 SP5, 15 SP1, 15 SP3, 15 SP3 SUSE Linux Enterprise High Performance Computing 12 SP5, 15 SP1, 15 SP2, 15 SP3, 15 SP4, 15 SP1 LTSS 15-SP1, 15 SP2 LTSS 15-SP2, 15 SP1 LTSS 15-SP1, ESPOS 15 SP3, LTSS 15 SP3 SUSE Linux Enterprise Live Patching 12-SP5, 15-SP1, 15-SP2, 15-SP3, 15-SP4 SUSE Linux Enterprise Micro 5.1, 5.2, 5.3, 5.4 SUSE Linux Enterprise Micro for Rancher 5.2, 5.3 SUSE Linux Enterprise Real Time 12 SP5 SUSE Linux Enterprise Real Time 15 SP3 SUSE Linux Enterprise Real Time 15 SP4 SUSE Linux Enterprise Server 12 SP5 SUSE Linux Enterprise Server 15 SP1, 15 SP2, 15 SP3, 15 SP4, 15 SP1 LTSS 15-SP1, 15 SP2 LTSS 15-SP2, 15 SP3 LTSS 15-SP3 SUSE Linux Enterprise Server 15 SP1 Business Critical Linux 15-SP1, SP2 Business Critical Linux 15-SP2, SP3 Business Critical Linux 15-SP3 SUSE Linux Enterprise Server for SAP Applications 12 SP5, 15 SP1, 15 SP2, 15 SP3, 15 SP4 SUSE Linux Enterprise Software Development Kit 12 SP5 SUSE Linux Enterprise Workstation Extension 12 12-SP5 SUSE Manager Proxy 4.0, 4.1, 4.2 SUSE Manager Retail Branch Server 4.0, 4.1, 4.2 SUSE Manager Server 4.0, 4.1, 4.2 SUSE Real Time Module 15-SP3, 15-SP4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2023/suse-su-20230747-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20230749-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20230762-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20230768-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20230770-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20230778-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20230779-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20230780-1/

Affected Product	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-47520, CVE-2022-3521, CVE-2022-42328, CVE-2022-3545, CVE-2022-47518, CVE-2022-47521, CVE-2022-3344, CVE-2022-3435, CVE-2023-26605, CVE-2022-4139, CVE-2022-47519, CVE-2022-42329, CVE-2023-0179, CVE-2022-45869, CVE-2022-4379, CVE-2022-3169, CVE-2023-0468, CVE-2023-0461, CVE-2017-11503, CVE-2021-3603, CVE-2016-10045, CVE-2017-5223, CVE-2016-10033, CVE-2018-19296, CVE-2020-13625)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could lead to Arbitrary code execution, Denial of service, Sensitive information disclosure, Cross-site Scripting. Ubuntu recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Ubuntu 16.0 Ubuntu 16.04 Ubuntu 18.04 Ubuntu 20.04 Ubuntu 22.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-5962-1 https://ubuntu.com/security/notices/USN-5956-2 https://ubuntu.com/security/notices/USN-5956-1

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.