



Advisory Alert

Alert Number: AAA20230717

Date: July 17, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

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

Description

Affected Product	Suse
Severity	High
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-1077, CVE-2023-1079, CVE-2023-1249, CVE-2023-1637, CVE-2023-1829, CVE-2023-2002, CVE-2023-21102, CVE-2023-3090, CVE-2023-3111, CVE-2023-3141, CVE-2023-3159, CVE-2023-3161, CVE-2023-3212, CVE-2023-3268, CVE-2023-3357, CVE-2023-3358, CVE-2023-3389, CVE-2023-35788, CVE-2023-35823, CVE-2023-35824, CVE-2023-35828, CVE-2023-35829)
Description	Suse has released security updates addressing multiple vulnerabilities that exist in their Products These vulnerabilities may result in a System crash, NULL pointer dereference, use-after-free Condition, Heap out-of-bounds write Suse recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Basesystem Module 15-SP4 Development Tools Module 15-SP4 Legacy Module 15-SP4 openSUSE Leap 15.4 openSUSE Leap 15.5 openSUSE Leap Micro 5.3 Public Cloud Module 15-SP4 SUSE CaaS Platform 4.0 SUSE Enterprise Storage 7 SUSE Linux Enterprise Desktop 15 SP4 SUSE Linux Enterprise High Availability Extension 12 SP5 SUSE Linux Enterprise High Availability Extension 15 SP1,SP2, SP4 SUSE Linux Enterprise High Performance Computing 12 SP5 SUSE Linux Enterprise High Performance Computing 15 SP1 LTSS 15-SP1 SUSE Linux Enterprise High Performance Computing 15 SP2 LTSS 15-SP2 SUSE Linux Enterprise High Performance Computing 15 SP4 SUSE Linux Enterprise Live Patching 12-SP5 SUSE Linux Enterprise Live Patching 15-SP1, SP2, SP4 SUSE Linux Enterprise Micro 5.3, 5.4 SUSE Linux Enterprise Micro for Rancher 5.3, 5.4 SUSE Linux Enterprise Real Time 15 SP4 SUSE Linux Enterprise Server 12 SP5 SUSE Linux Enterprise Server 15 SP1 SUSE Linux Enterprise Server 15 SP1 Business Critical Linux 15-SP1 SUSE Linux Enterprise Server 15 SP1 LTSS 15-SP1 SUSE Linux Enterprise Server 15 SP2 SUSE Linux Enterprise Server 15 SP2 Business Critical Linux 15-SP2 SUSE Linux Enterprise Server 15 SP2 LTSS 15-SP2 SUSE Linux Enterprise Server 15 SP4 SUSE Linux Enterprise Server for SAP Applications 12 SP5 , 15 SP1, 15 SP2, 15 SP4 SUSE Linux Enterprise Software Development Kit 12 SP5 SUSE Linux Enterprise Workstation Extension 12 12-SP5 SUSE Linux Enterprise Workstation Extension 15 SP4 SUSE Manager Proxy 4.0, 4.1, 4.3 SUSE Manager Retail Branch Server 4.0, 4.1, 4.3 SUSE Manager Server 4.0, 4.1, 4.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2023/suse-su-20232834-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20232831-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20232830-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20232822-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20232820-1/

Affected Product	Ubuntu
Severity	High, Low
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-3212, CVE-2023-3141, CVE-2023-31084, CVE-2023-2124, CVE-2023-3090)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in their Products. These vulnerabilities may result in a denial of service and arbitrary code execution. Ubuntu recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Ubuntu 22.04 LTS
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-6231-1

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.