Advisory Alert

Alert Number: AAA20231207 **Date:** December 7, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

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

Description

Affected Product	**Suse**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-26345, CVE-2021-46766, CVE-2021-46774, CVE-2022-23820, CVE-2022-23830, CVE-2023-20519, CVE-2023-20521, CVE-2023-20526, CVE-2023-20533, CVE-2023-20566)
Description	Suse has released security updates addressing multiple vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could lead to denial of service, arbitrary code execution, privilege escalation Suse recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Basesystem Module 15-SP4 Basesystem Module 15-SP5 openSUSE Leap 15.3, 15.4, 15.5 openSUSE Leap Micro 5.3, Micro 5.4 SUSE CaaS Platform 4.0 SUSE Enterprise Storage 7.1 SUSE Linux Enterprise Desktop 15 SP4 ,SP5 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 SP3 SUSE Linux Enterprise High Performance Computing 15 SP4 SUSE Linux Enterprise High Performance Computing 15 SP5 SUSE Linux Enterprise High Performance Computing ESPOS 15 SP3 SUSE Linux Enterprise High Performance Computing LTSS 15 SP3 SUSE Linux Enterprise Micro 5.1 to 5.5 SUSE Linux Enterprise Micro for Rancher 5.2, 5.3, 5.4 SUSE Linux Enterprise Real Time 15 SP4 SUSE Linux Enterprise Real Time 15 SP5 SUSE Linux Enterprise Server 12 SP5 SUSE Linux Enterprise Server 15 SP1 LTSS 15-SP1 SUSE Linux Enterprise Server 15 SP2 LTSS 15-SP2 SUSE Linux Enterprise Server 15 SP3 LTSS 15-SP3 SUSE Linux Enterprise Server 15 SP4, SP5 SUSE Linux Enterprise Server for SAP Applications 12 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP1, SP2, SP3, SP4, SP5 SUSE Manager Proxy 4.3 SUSE Manager Retail Branch Server 4.3 SUSE Manager Server 4.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2023/suse-su-20234660-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20234664-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20234665-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20234654-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20234655-1/

Affected Product	**Lenovo**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-5058, CVE-2023-39538, CVE-2023-39539, CVE-2023-40238)
Description	Lenovo has released a security update addressing multiple vulnerabilities that exist in the image parsing libraries in AMI, Insyde and Phoenix BIOS which are used to parse personalized boot logos that are loaded from the EFI System Partition that could allow a local attacker with elevated privileges to trigger a denial of service or arbitrary code execution. Lenovo recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Multiple Lenovo products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.lenovo.com/us/en/product_security/LEN-145284

Affected Product	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-5158, CVE-2023-5178, CVE-2023-4244, CVE-2023-5633, CVE-2023-5345, CVE-2023-45898, CVE-2023-5090, CVE-2023-5717, CVE-2023-39189, CVE-2023-42754, CVE-2023-31085)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could lead to denial of service , NULL pointer dereference , information disclosure, local privilege escalation Ubuntu recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Ubuntu 23.10 Ubuntu 22.04 LTS
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-6536-1 https://ubuntu.com/security/notices/USN-6537-1

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.