TLP: WHITE

Advisory Alert

Alert Number: AAA20230920 **Date:** September 20, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Suse	**High**	Kernel Security Updates
Ubuntu	**High**, **Medium**, **Low**	Multiple vulnerabilities

Description

Affected Product	**Suse**
Severity	**High**
Affected Vulnerability	Kernel Security Updates (CVE-2022-36402, CVE-2023-2007, CVE-2023-20588, CVE-2023-21400, CVE-2023-3772, CVE-2023-3863, CVE-2023-4128, CVE-2023-4132, CVE-2023-4134, CVE-2023-4273, CVE-2023-4385, CVE-2023-4387, CVE-2023-4459)
Description	Suse has released a security update addressing Linux Kernel Security updates affecting their products. Exploitation of these vulnerabilities could lead multiple security flows. Suse recommends to apply the necessary security fixes at your earliest to avoid issues
Affected Products	SUSE Linux Enterprise High Availability Extension 15 SP2 SUSE Linux Enterprise High Performance Computing 15 SP2 SUSE Linux Enterprise High Performance Computing 15 SP2 LTSS 15-SP2 SUSE Linux Enterprise Live Patching 15-SP2 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 for SAP Applications 15 SP2 SUSE Manager Proxy 4.1 SUSE Manager Retail Branch Server 4.1 SUSE Manager Server 4.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2023/suse-su-20233687-1/

Affected Product	**Ubuntu**
Severity	**High** , **Medium** , **Low**
Affected Vulnerability	Multiple vulnerabilities (CVE-2023-20588, CVE-2023-40283, CVE-2023-4128, CVE-2023-4569, CVE-2022-40982, CVE-2023-3212, CVE-2023-32269, CVE-2023-3863, CVE-2023-4385, CVE-2023-4387, CVE-2023-4459)
Description	Ubuntu has released security updates addressing Multiple Vulnerabilities. If exploited, these Vulnerabilities could lead to sensitive information disclosure, privilege escalation, Use-after-free, Memory leak and denial of service Ubuntu recommends to apply the necessary security fixes at your earliest to avoid issues.
Affected Products	Ubuntu 22.04 Ubuntu 20.04 Ubuntu 16.04 Ubuntu 14.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-6386-1 https://ubuntu.com/security/notices/USN-6387-1 https://ubuntu.com/security/notices/USN-6388-1

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.