Advisory Alert

Alert Number: AAA20231003 **Date:** October 3, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Suse	**High**	Multiple Vulnerabilities

Description

Affected Product	**Suse**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-4273, CVE-2023-3609, CVE-2023-3776, CVE-2023-31248, CVE-2023-1829, CVE-2023-3812)
Description	Suse has released security updates addressing multiple vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could lead to Stack overflow, Use-after-free condition, Privilege escalation and System crash. Suse recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	openSUSE Leap 15.4, 15.5 SUSE Linux Enterprise High Performance Computing 15 SP3, 15 SP4, 15 SP5 SUSE Linux Enterprise Live Patching 15-SP3, 15-SP4, 15-SP5 SUSE Linux Enterprise Micro 5.1, 5.2, 5.3, 5.4, 5.5 SUSE Linux Enterprise Real Time 15 SP4, 15 SP5 SUSE Linux Enterprise Server 15 SP3, 15 SP4, 15 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP3, 15 SP4, 15 SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2023/suse-su-20233929-1 https://www.suse.com/support/update/announcement/2023/suse-su-20233924-1 https://www.suse.com/support/update/announcement/2023/suse-su-20233923-1 https://www.suse.com/support/update/announcement/2023/suse-su-20233922-1 https://www.suse.com/support/update/announcement/2023/suse-su-20233912-1 https://www.suse.com/support/update/announcement/2023/suse-su-20233928-1

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.