Advisory Alert

Alert Number: **AAA20230718** **Date:** **July 18, 2023**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Suse	**High**	Multiple Vulnerabilities
OpenSSL	**Low**	Improper Authentication Vulnerability

Description

Affected Product	**Suse**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-1077, CVE-2023-1249, CVE-2023-2002, CVE-2023-3090, CVE-2023-3141, CVE-2023-3159, CVE-2023-3161, CVE-2023-3268, CVE-2023-3358, CVE-2023-35788, CVE-2023-35823, CVE-2023-35824, CVE-2023-35828)
Description	Suse has a released security update addressing multiple vulnerabilities affecting their products. Exploitation of these vulnerabilities could lead to Heap out-of-bounds write, Use-after-free flaw, NULL pointer dereference. Suse recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	openSUSE Leap 15.4 SUSE Enterprise Storage 7.1 SUSE Linux Enterprise High Availability Extension 15 SP3 SUSE Linux Enterprise High Performance Computing 15 SP3 SUSE Linux Enterprise High Performance Computing ESPOS 15 SP3 SUSE Linux Enterprise High Performance Computing LTSS 15 SP3 SUSE Linux Enterprise Live Patching 15-SP3 SUSE Linux Enterprise Micro 5.1, 5.2 SUSE Linux Enterprise Micro for Rancher 5.2 SUSE Linux Enterprise Real Time 15 SP3 SUSE Linux Enterprise Server 15 SP3 SUSE Linux Enterprise Server 15 SP3 Business Critical Linux 15-SP3 SUSE Linux Enterprise Server 15 SP3 LTSS 15-SP3 SUSE Linux Enterprise Server for SAP Applications 15 SP3 SUSE Manager Proxy 4.2 SUSE Manager Retail Branch Server 4.2 SUSE Manager Server 4.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2023/suse-su-20232859-1/

Affected Product	**OpenSSL**
Severity	**Low**
Affected Vulnerability	Improper Authentication Vulnerability (CVE-2023-2975)
Description	OpenSSL has released a patch update addressing an Improper Authentication Vulnerability that exists within the AES-SIV cipher implementation. The flaw causes it to ignore empty associated data entries which are unauthenticated as a consequence. OpenSSL recommends to apply the available patch updates at your earliest to avoid issues.
Affected Products	OpenSSL versions 3.0.0 to 3.0.9, and 3.1.0 to 3.1.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.openssl.org/news/secadv/20230714.txt

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.