Advisory Alert

Alert Number: AAA20251230 **Date:** December 30, 2025

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-2022-50280, CVE-2023-53659, CVE-2023-53676, CVE-2023-53717, CVE-2025-40040, CVE-2025-40121, CVE-2025-40154, CVE-2025-40204)
Description	SUSE has released a security update addressing multiple vulnerabilities that exists in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. SUSE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	openSUSE Leap 15.3 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 LTSS 15 SP3 SUSE Linux Enterprise Live Patching 15-SP3 SUSE Linux Enterprise Micro 5.1 SUSE Linux Enterprise Micro 5.2 SUSE Linux Enterprise Micro for Rancher 5.2 SUSE Linux Enterprise Server 15 SP3 SUSE Linux Enterprise Server 15 SP3 Business Critical Linux SUSE Linux Enterprise Server 15 SP3 LTSS 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/2025/suse-su-20254530-1/

Disclaimer

The information provided are gathered from official service provider's websites and portals. FinCSIRT strongly recommends members to apply security fixes as per the given guidelines, following the organization's patch and change management procedures to protect systems from potential threats.