Advisory Alert

Alert Number: AAA20251226 **Date:** December 26, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SUSE	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**SUSE**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-50253, CVE-2023-53676, CVE-2025-21710, CVE-2025-37916, CVE-2025-38359, CVE-2025-38361, CVE-2025-39788, CVE-2025-39805, CVE-2025-39819, CVE-2025-39859, CVE-2025-39944, CVE-2025-39980, CVE-2025-40001, CVE-2025-40021, CVE-2025-40027, CVE-2025-40030, CVE-2025-40038, CVE-2025-40040, CVE-2025-40048, CVE-2025-40055, CVE-2025-40059, CVE-2025-40064, CVE-2025-40070, CVE-2025-40074, CVE-2025-40075, CVE-2025-40083, CVE-2025-40098, CVE-2025-40105, CVE-2025-40107, CVE-2025-40109, CVE-2025-40110, CVE-2025-40111, CVE-2025-40115, CVE-2025-40116, CVE-2025-40118, CVE-2025-40120, CVE-2025-40121, CVE-2025-40127, CVE-2025-40129, CVE-2025-40139, CVE-2025-40140, CVE-2025-40141, CVE-2025-40149, CVE-2025-40159, CVE-2025-40168, CVE-2025-40169, CVE-2025-40173, CVE-2025-40176, CVE-2025-40180, CVE-2025-40183, CVE-2025-40186, CVE-2025-40188, CVE-2025-40194, CVE-2025-40198, CVE-2025-40200, CVE-2025-40204, CVE-2025-40205, CVE-2025-40206, CVE-2025-40207)
Description	SUSE has released a security update addressing multiple vulnerabilities that exist in the Linux kernel for SUSE Products. These vulnerabilities could be exploited by malicious users to cause a Denial of Service, unauthorized disclosure of sensitive kernel memory, or potential elevation of privileges. SUSE advises applying these security fixes and rebooting affected systems at your earliest convenience to protect against potential threats and ensure system stability.
Affected Products	openSUSE Leap 15.6 SUSE Linux Enterprise Live Patching 15-SP6 SUSE Linux Enterprise Real Time 15 SP6 SUSE Linux Enterprise Server 15 SP6 SUSE Linux Enterprise Server for SAP Applications 15 SP6 SUSE Real Time Module 15-SP6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2025/suse-su-20254521-1/

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.