Advisory Alert

Alert Number: AAA20241129 **Date:** November 29, 2024

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
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
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 SUSE Linux Enterprise Live Patching 15-SP2 SUSE Linux Enterprise Server 15 SP2 SUSE Linux Enterprise Server 15 SP2 Business Critical Linux SUSE Linux Enterprise Server 15 SP2 LTSS 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 SUSE Linux Enterprise High Availability Extension 12 SP5 SUSE Linux Enterprise High Performance Computing 12 SP5 SUSE Linux Enterprise Live Patching 12-SP5 SUSE Linux Enterprise Server 12 SP5 SUSE Linux Enterprise Server 12 SP5 LTSS SUSE Linux Enterprise Server 12 SP5 LTSS Extended Security SUSE Linux Enterprise Server for SAP Applications 12 SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2024/suse-su-20244100-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20244103-1/

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.