Advisory Alert

Alert Number: AAA20250218 **Date:** February 18, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SUSE	**High**	Multiple Linux Kernel Vulnerabilities

Description

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Linux Kernel Vulnerabilities (CVE-2021-47222, CVE-2021-47223, CVE-2024-26644, CVE-2024-47809, CVE-2024-48881, CVE-2024-49948, CVE-2024-50142, CVE-2024-52332, CVE-2024-53155, CVE-2024-53185, CVE-2024-53197, CVE-2024-53227, CVE-2024-55916, CVE-2024-56369, CVE-2024-56532, CVE-2024-56533, CVE-2024-56539, CVE-2024-56574, CVE-2024-56593, CVE-2024-56594, CVE-2024-56600, CVE-2024-56601, CVE-2024-56615, CVE-2024-56623, CVE-2024-56630, CVE-2024-56637, CVE-2024-56641, CVE-2024-56643, CVE-2024-56650, CVE-2024-56661, CVE-2024-56662, CVE-2024-56681, CVE-2024-56700, CVE-2024-56722, CVE-2024-56739, CVE-2024-56747, CVE-2024-56748, CVE-2024-56759, CVE-2024-56763, CVE-2024-56769, CVE-2024-57884, CVE-2024-57890, CVE-2024-57896, CVE-2024-57899, CVE-2024-57903, CVE-2024-57922, CVE-2024-57929, CVE-2024-57931, CVE-2024-57932, CVE-2024-57938, CVE-2025-21653, CVE-2025-21664, CVE-2025-21678, CVE-2025-21682, CVE-2024-40980, CVE-2024-46858, CVE-2024-49978, CVE-2024-50251, CVE-2024-50258, CVE-2024-50304, CVE-2024-53123, CVE-2024-53187, CVE-2024-53203, CVE-2024-56592, CVE-2024-56608, CVE-2024-56610, CVE-2024-56633, CVE-2024-56658, CVE-2024-56665, CVE-2024-56679, CVE-2024-56693, CVE-2024-56707, CVE-2024-56715, CVE-2024-56725, CVE-2024-56726, CVE-2024-56727, CVE-2024-56728, CVE-2024-57802, CVE-2024-57882, CVE-2024-57917, CVE-2024-57946, CVE-2025-21652, CVE-2025-21655, CVE-2025-21663, CVE-2025-21665, CVE-2025-21666, CVE-2025-21667, CVE-2025-21668, CVE-2025-21669, CVE-2025-21670, CVE-2025-21673, CVE-2025-21674, CVE-2025-21675, CVE-2025-21676, CVE-2025-21681)
Description	SUSE has released security updates addressing Multiple Linux Kernel Vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Use-after-free, integer overflow, Memory leak, NULL pointer dereference. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Confidential Computing Module 15-SP6 SUSE Linux Enterprise Server 15 SP6 SUSE Linux Enterprise Server for SAP Applications 15 SP6 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/2025/suse-su-20250565-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20250564-1/

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.