Advisory Alert

Alert Number: AAA20250523 **Date:** May 23, 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-2023-53034, CVE-2024-27018, CVE-2024-27415, CVE-2024-28956, CVE-2024-35840, CVE-2024-43882, CVE-2024-46763, CVE-2024-46865, CVE-2024-50038, CVE-2024-50083, CVE-2024-50115, CVE-2024-50162, CVE-2024-50163, CVE-2024-53042, CVE-2024-53124, CVE-2024-53139, CVE-2024-53156, CVE-2024-56641, CVE-2024-56702, CVE-2024-57924, CVE-2024-57998, CVE-2024-58001, CVE-2024-58018, CVE-2024-58068, CVE-2024-58070, CVE-2024-58071, CVE-2024-58088, CVE-2024-58093, CVE-2024-58094, CVE-2024-58095, CVE-2024-58096, CVE-2024-58097, CVE-2025-21683, CVE-2025-21696, CVE-2025-21707, CVE-2025-21729, CVE-2025-21755, CVE-2025-21758, CVE-2025-21768, CVE-2025-21792, CVE-2025-21806, CVE-2025-21808, CVE-2025-21812, CVE-2025-21833, CVE-2025-21836, CVE-2025-21852, CVE-2025-21853, CVE-2025-21854, CVE-2025-21863, CVE-2025-21867, CVE-2025-21873, CVE-2025-21875, CVE-2025-21881, CVE-2025-21884, CVE-2025-21887, CVE-2025-21889, CVE-2025-21894, CVE-2025-21895, CVE-2025-21904, CVE-2025-21905, CVE-2025-21906, CVE-2025-21908, CVE-2025-21909, CVE-2025-21910, CVE-2025-21912, CVE-2025-21913, CVE-2025-21914, CVE-2025-21915, CVE-2025-21916, CVE-2025-21917, CVE-2025-21918, CVE-2025-21922, CVE-2025-21923, CVE-2025-21924, CVE-2025-21925, CVE-2025-21926, CVE-2025-21927, CVE-2025-21928, CVE-2025-21930, CVE-2025-21931, CVE-2025-21934, CVE-2025-21935, CVE-2025-21936, CVE-2025-21937, CVE-2025-21941, CVE-2025-21943, CVE-2025-21948, CVE-2025-21950, CVE-2025-21951, CVE-2025-21953, CVE-2025-21956, CVE-2025-21957, CVE-2025-21960, CVE-2025-21961, CVE-2025-21962, CVE-2025-21963, CVE-2025-21964, CVE-2025-21966, CVE-2025-21968, CVE-2025-21969, CVE-2025-21970, CVE-2025-21971, CVE-2025-21972, CVE-2025-21975, CVE-2025-21978, CVE-2025-21979, CVE-2025-21980, CVE-2025-21981, CVE-2025-21985, CVE-2025-21991, CVE-2025-21992, CVE-2025-21993, CVE-2025-21995, CVE-2025-21996, CVE-2025-21999, CVE-2025-22001, CVE-2025-22003, CVE-2025-22004, CVE-2025-22007, CVE-2025-22008, CVE-2025-22009, CVE-2025-22010, CVE-2025-22013, CVE-2025-22014, CVE-2025-22015, CVE-2025-22016, CVE-2025-22017, CVE-2025-22018, CVE-2025-22020, CVE-2025-22025, CVE-2025-22027, CVE-2025-22029, CVE-2025-22033, CVE-2025-22036, CVE-2025-22044, CVE-2025-22045, CVE-2025-22050, CVE-2025-22053, CVE-2025-22055, CVE-2025-22058, CVE-2025-22060, CVE-2025-22062, CVE-2025-22064, CVE-2025-22065, CVE-2025-22075, CVE-2025-22080, CVE-2025-22086, CVE-2025-22088, CVE-2025-22090, CVE-2025-22093, CVE-2025-22097, CVE-2025-22102, CVE-2025-22104, CVE-2025-22105, CVE-2025-22106, CVE-2025-22107, CVE-2025-22108, CVE-2025-22109, CVE-2025-22115, CVE-2025-22116, CVE-2025-22121, CVE-2025-22128, CVE-2025-2312, CVE-2025-23129, CVE-2025-23131, CVE-2025-23133, CVE-2025-23136, CVE-2025-23138, CVE-2025-23145, CVE-2025-37785, CVE-2025-37798, CVE-2025-37799, CVE-2025-37860, CVE-2025-39728)
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in SUSE Linux Kernel. These vulnerabilities could be exploited by malicious users to cause memory leak, Use-after-free, NULL pointer dereference, Out-of-bound read. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Basesystem Module 15-SP6 Development Tools Module 15-SP6 Legacy Module 15-SP6 OpenSUSE Leap 15.3, 15.4, 15.5, 15.6 SUSE Linux Enterprise Desktop 15 SP6 SUSE Linux Enterprise High Availability Extension 15 SP6 SUSE Linux Enterprise High Performance Computing 12 SP5, 15 SP3, 15 SP4, 15 SP5 SUSE Linux Enterprise Live Patching 12-SP5 SUSE Linux Enterprise Live Patching 15-SP3, 15-SP4, 15-SP5, 15-SP6 SUSE Linux Enterprise Micro 5.1, 5.2, 5.3, 5.4, 5.5 SUSE Linux Enterprise Real Time 15 SP4, 15 SP5, 15 SP6 SUSE Linux Enterprise Server 12 SP5, 15 SP3, 15 SP4, 15 SP5, 15 SP6 SUSE Linux Enterprise Server for SAP Applications 12 SP5, 15 SP3, 15 SP4, 15 SP5, 15 SP6 SUSE Linux Enterprise Workstation Extension 15 SP6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2025/suse-su-202501610-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202501611-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202501614-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202501652-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202501655-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202501656-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202501663-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202501669-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202501672-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202501668-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202501675-1/

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.