Advisory Alert

Alert Number: AAA20241218 **Date:** December 18, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SUSE	**High**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Red Hat	**Medium**	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 couse Memory Leaks, Use After Free, Out-of-bounds Read, Buffer Overflow. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Basesystem Module 15-SP5 Development Tools Module 15-SP5 Legacy Module 15-SP5 openSUSE Leap 15.4 SUSE Linux Enterprise Desktop 15 SP4 LTSS, 15 SP5 SUSE Linux Enterprise High Availability Extension 12 SP5, 15 SP4, 15 SP5 SUSE Linux Enterprise High Performance Computing 12 SP5, 15 SP4, 15 SP5 SUSE Linux Enterprise High Performance Computing ESPOS 15 SP4, LTSS 15 SP4 SUSE Linux Enterprise Live Patching 12-SP5, 15-SP4, 15-SP5 SUSE Linux Enterprise Micro 5.3, 5.4, 5.5 SUSE Linux Enterprise Micro for Rancher 5.3, 5.4 SUSE Linux Enterprise Real Time 15 SP4, 15 SP5 SUSE Linux Enterprise Server 12 SP5, 12 SP5 LTSS SUSE Linux Enterprise Server 12 SP5 LTSS Extended Security SUSE Linux Enterprise Server 15 SP4, 15 SP4 LTSS SUSE Linux Enterprise Server 15 SP5 SUSE Linux Enterprise Server for SAP Applications 12 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP4 SUSE Linux Enterprise Server for SAP Applications 15 SP5 SUSE Manager Proxy 4.3 SUSE Manager Retail Branch Server 4.3 SUSE Manager Server 4.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2024/suse-su-20244345-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20244346-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20244364-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20244367-1

Affected Product	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	Ubuntu has released security updates addressing multiple vulnerabilities in their products. These vulnerabilities could be exploited by malicious users to compromise the Affected System. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 18.04 Ubuntu 20.04 Ubuntu 22.04 Ubuntu 24.04 Ubuntu 24.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://ubuntu.com/security/notices/USN-7166-1 • https://ubuntu.com/security/notices/USN-7167-1 • https://ubuntu.com/security/notices/USN-7169-1 • https://ubuntu.com/security/notices/USN-7173-1

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-47384, CVE-2024-38627, CVE-2024-39499, CVE-2024-40989)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to NULL Pointer Dereference, Double Free, Speculation Leaks. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.4 x86_64 Red Hat Enterprise Linux Server - AUS 9.4 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.4 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.4 aarch64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.4 x86_64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.4 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.4 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.4 aarch64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.4 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.4 s390x Red Hat Enterprise Linux for Real Time for x86_64 - 4 years of updates 9.4 x86_64 Red Hat Enterprise Linux for Real Time for NFV for x86_64 - 4 years of updates 9.4 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2024:11313

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.