Advisory Alert

Alert Number: **AAA20240216** **Date:** **February 16, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-4921, CVE-2024-0646)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause out of bounds write and use-after-free condition. **CVE-2023-4921-** A use-after-free flaw was found in qfq_dequeue and agg_dequeue in net/sched/sch_qfq.c in the Traffic Control (QoS) subsystem in the Linux kernel. This issue may allow a local user to crash the system or escalate their privileges on the system. **CVE-2024-0646-** An out-of-bounds memory write flaw was found in the Linux kernel's Transport Layer Security functionality in how a user calls a function splice with a ktls socket as the destination. This flaw allows a local user to crash or potentially escalate their privileges on the system. Red Hat recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.2 x86_64, 8.6 x86_64 Red Hat Enterprise Linux Server - AUS 9.2 x86_64, AUS 8.6 x86_64 Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.2 ppc64le, 8.6 ppc64le Red Hat Enterprise Linux Server - TUS 8.6 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.2 x86_64, 8.6 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2024:0850 https://access.redhat.com/errata/RHSA-2024:0851

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-33631, CVE-2023-46838, CVE-2023-47233, CVE-2023-4921, CVE-2023-51043, CVE-2023-51780, CVE-2023-51782, CVE-2023-6040, CVE-2023-6356, CVE-2023-6535, CVE-2023-6536, CVE-2023-6915, CVE-2024-0565, CVE-2024-0775, CVE-2024-1086)
Description	SUSE has released security updates addressing multiple vulnerabilities in the SUSE Linux Kernel. If exploited, these vulnerabilities could lead to escalation of privilege, information leak. SUSE recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	SUSE Linux Enterprise High Availability Extension 15 SP2 SUSE Linux Enterprise High Performance Computing 15 SP2 SUSE Linux Enterprise High Performance Computing LTSS 15-SP2 SUSE Linux Enterprise Live Patching 15-SP2 SUSE Linux Enterprise Server 15 SP2 SUSE Linux Enterprise Server 15 SP2 Business Critical Linux 15-SP2 SUSE Linux Enterprise Server 15 SP2 LTSS 15-SP2 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
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2024/suse-su-20240478-1/

Affected Product	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-6531, CVE-2023-51780, CVE-2023-6932, CVE-2024-22705, CVE-2023-51781, CVE-2024-0646, CVE-2023-51782, CVE-2024-0565, CVE-2023-6121, CVE-2024-0607, CVE-2023-6622, CVE-2023-6039, CVE-2023-32252, CVE-2023-32257, CVE-2023-32250, CVE-2023-6931, CVE-2024-0193, CVE-2023-35827, CVE-2023-6176, CVE-2023-6817, CVE-2023-46813, CVE-2023-6040, CVE-2023-6606, CVE-2023-34324, CVE-2024-0641)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exists in Ubuntu Linux kernel. If exploited, these could allow a remote attacker to cause escalation of privilege, sensitive information disclosure, arbitrary code execution and denial of service It is recommended by Ubuntu to apply necessary security fixes at earliest to avoid issues.
Affected Products	Ubuntu 22.04 LTS Ubuntu 20.04 LTS
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-6639-1 https://ubuntu.com/security/notices/USN-6628-2

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.