Advisory Alert

Alert Number: AAA20230328 **Date:** March 28, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Redhat	**High**	Multiple Vulnerabilities
Suse	**High**	Multiple Vulnerabilities
Citrix	**High**	Improper Access Control vulnerability
Ubuntu	**High**, Medium, Low	Multiple Vulnerabilities

Description

Affected Product	**Redhat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-4744, CVE-2023-0266, CVE-2022-4269)
Description	Redhat has release security updates addressing Multiple Vulnerabilities that exist in their products. If exploited these vulnerabilities could lead to denial of service and Privilege escalation. **CVE-2022-4744-** Privilege escalation vulnerability in Linux kernel's TUN/TAP device driver. Flaw in register_netdevice function allows a local user to crash or potentially escalate their privileges on the system. **CVE-2023-0266-** A use-after-free flaw was found in the ALSA subsystem in sound/core/control.c in the Linux kernel. This flaw allows a local attacker to cause a use-after-free issue. **CVE-2022-4269-** Denial of service vulnerability in Linux kernel Traffic Control (TC) subsystem A local user can use a specific network configuration to trigger a CPU soft lockup. Redhat recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Red Hat CodeReady Linux Builder for ARM 64 9 aarch64 - Extended Update Support 9.0 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems 9 s390x - Extended Update Support 9.0 s390x Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.0 ppc64le Red Hat CodeReady Linux Builder for Power, little endian 9 ppc64le Red Hat CodeReady Linux Builder for x86_64 9 x86_64 - Extended Update Support 9.0 x86_64 Red Hat Enterprise Linux for ARM 64 9 aarch64 - Extended Update Support 9.0 aarch64 Red Hat Enterprise Linux for IBM z Systems 9 s390x - Extended Update Support 9.0 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.0 ppc64le Red Hat Enterprise Linux for Power, little endian 9 ppc64le Red Hat Enterprise Linux for Real Time 9 x86_64 Red Hat Enterprise Linux for Real Time for NFV 9 x86_64 Red Hat Enterprise Linux for Real Time for NFV for x86_64 - 4 years of updates 9.0 x86_64 Red Hat Enterprise Linux for Real Time for x86_64 - 4 years of updates 9.0 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.0 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.0 x86_64 Red Hat Enterprise Linux for x86_64 9 x86_64 Red Hat Enterprise Linux Server for ARM 64 - 4 years of updates 9.0 aarch64 Red Hat Enterprise Linux Server for IBM z Systems - 4 years of updates 9.0 s390x Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.0 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2023:1471 https://access.redhat.com/errata/RHSA-2023:1470 https://access.redhat.com/errata/RHSA-2023:1469 https://access.redhat.com/errata/RHSA-2023:1468 https://access.redhat.com/errata/RHSA-2023:1467

Affected Product	**Citrix**
Severity	**High**
Affected Vulnerability	Improper Access Control vulnerability (CVE-2023-24486)
Description	Citrix has release a security update addressing Improper Access Control vulnerability that exist in Citrix Workspace app for Linux. If exploited, a local malicious user would be able to gain access to the Citrix Virtual Apps and Desktops session of another user who is using the same computer from which the ICA session is launched. Citrix recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Citrix Workspace App
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/article/CTX477618/citrix-workspace-app-for-linux-security-bulletin-for-cve202324486

Affected Product	**Suse**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-0266 ,CVE-2023-1078 ,CVE-2023-26545)
Description	Suse has release security updates addressing Multiple Vulnerabilities that exist in their products. If exploited these vulnerabilities could lead to heap out-of-bounds write condition, use-after-free and double free condition. **CVE-2023-0266 –** The vulnerability exists due to an use-after-free error within the snd_ctl_elem_read() function. A local user can trigger a use-after-free error and perform a denial of service attack. **CVE-2023-1078 -** The vulnerability exists due to a boundary error within the rds_rm_zerocopy_callback() function in Linux kernel RDS (Reliable Datagram Sockets) protocol. A local user can trigger an out-of-bounds write and execute arbitrary code with elevated privileges. **CVE-2023-26545-** The vulnerability exists due to a double free in net/mpls/af_mpls.c during the renaming of a device. A local user can trigger a double free error and execute arbitrary code with elevated privileges. Suse recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	SUSE Linux Enterprise High Performance Computing 15 SP1, SP2, SP3, SP4 SUSE Linux Enterprise Live Patching 15-SP1, SP2, SP3, SP4 SUSE Linux Enterprise Micro 5.1, Micro 5.2, Micro 5.3, Micro 5.4 SUSE Linux Enterprise Real Time 15 SP4 SUSE Linux Enterprise Server 15 SP1, SP2, SP3, SP4 SUSE Linux Enterprise Server for SAP Applications 15 SP1, SP2, SP3, SP4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2023/suse-su-20231592-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20231588-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20231591-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20231574-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20231576-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20231579-1/

Affected Product	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-3669, CVE-2022-20369, CVE-2022-2196, CVE-2022-26373, CVE-2022-2663, CVE-2022-27672, CVE-2022-29900, CVE-2022-29901, CVE-2022-3061, CVE-2022-3424, CVE-2022-3521, CVE-2022-3545, CVE-2022-3628, CVE-2022-36280, CVE-2022-3640, CVE-2022-3646, CVE-2022-3649, CVE-2022-39842, CVE-2022-41218, CVE-2022-41849, CVE-2022-41850, CVE-2022-42328, CVE-2022-42329, CVE-2022-42895, CVE-2022-43750, CVE-2022-4382, CVE-2022-47929, CVE-2022-4842, CVE-2023-0045, CVE-2023-0179, CVE-2023-0266, CVE-2023-0394, CVE-2023-0461, CVE-2023-1032, CVE-2023-1073, CVE-2023-1074, CVE-2023-1075, CVE-2023-1078, CVE-2023-1281, CVE-2023-23455, CVE-2023-23559, CVE-2023-26545, CVE-2023-26607, CVE-2023-28328)
Description	Ubuntu has release security updates addressing Multiple Vulnerabilities that exist in their products. If exploited these vulnerabilities could lead to Denial of Service, use-after-free condition, Sensitive information disclosure, and arbitrary code execution. Ubuntu recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Ubuntu 16.04 ESM Ubuntu 18.04 LTS Ubuntu 20.04 LTS Ubuntu 22.04 LTS
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-5978-1 https://ubuntu.com/security/notices/USN-5977-1 https://ubuntu.com/security/notices/USN-5976-1 https://ubuntu.com/security/notices/USN-5975-1 https://ubuntu.com/security/notices/LSN-0093-1

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.