TLP: WHITE

Advisory Alert

Alert Number: **AAA20231109** **Date:** **November 9, 2023**

Document Classification Level **:** Public Circulation Permitted | Public

Information Classification Level **:** TLP: WHITE

Overview

Product	Severity	Vulnerability
Red hat	**High**	Multiple Vulnerabilities

Description

Affected Product	**Red hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-1095, CVE-2023-3609, CVE-2023-3776, CVE-2023-3812)
Description	Red hat has released security updates addressing multiple vulnerabilities within their products. **CVE-2023-1095** - A NULL pointer dereference flaw was found in the Linux kernel's netfilter subsystem. The issue could occur due to an error in nf_tables_updtable while freeing a transaction object not placed on the list head. This flaw allows a local, unprivileged user to crash the system, resulting in a denial of service. **CVE-2023-3609** - A Double-free flaw was found in u32_set_parms in net/sched/cls_u32.c in the Network Scheduler component in the Linux kernel. This flaw allows a local attacker to use a failure event to mishandle the reference counter, leading to a local privilege escalation threat. **CVE-2023-3776** - A Use-after-free vulnerability was found in fw_set_parms in net/sched/cls_fw.c in network scheduler sub-component in the Linux Kernel. This issue occurs due to a missing sanity check during cleanup at the time of failure, leading to a misleading reference. This may allow a local attacker to gain local privilege escalation. **CVE-2023-3812** - An Out-of-bounds memory access flaw was found in the Linux kernel's TUN/TAP device driver functionality in how a user generates a malicious (too big) networking packet when napi frags is enabled. This flaw allows a local user to crash or potentially escalate their privileges on the system. Redhat recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.1 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.1 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2023:6813 https://access.redhat.com/errata/RHSA-2023:6799

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.