Advisory Alert

Alert Number: AAA20250917 **Date:** September 17, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
Ubuntu	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-38052, CVE-2025-38352)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in Red Hat Enterprise Linux kernel. **CVE-2025-38052** - By manipulating the lifecycle of network namespaces, an attacker could exploit this vulnerability to cause a system crash or leak sensitive system memory. Exploitation of this vulnerability requires that a user has access to the system and the ability to create or destroy network namespaces. **CVE-2025-38352** - A race condition was found in the Linux kernel's POSIX CPU timer handling, where handle_posix_cpu_timers() may run concurrently with posix_cpu_timer_del() on an exiting task which could result in use-after-free scenarios. An attacker with local user access could use this flaw to crash or escalate their privileges on a system. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat Enterprise Linux for Power, little endian 8 ppc64le Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.4 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support Extension 8.8 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.8 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 - Update Services for SAP Solutions 9.2 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.4 x86_64 Red Hat Enterprise Linux for x86_64 8 x86_64 Red Hat Enterprise Linux Server - AUS 9.2 x86_64, AUS 9.4 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.8 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.0 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:16008 • https://access.redhat.com/errata/RHSA-2025:15933 • https://access.redhat.com/errata/RHSA-2025:15932 • https://access.redhat.com/errata/RHSA-2025:15931 • https://access.redhat.com/errata/RHSA-2025:15921

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-38742, CVE-2025-38743)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in Dell iDRAC Service Module. **CVE-2025-38742** - Dell iDRAC Service Module (iSM), version 6.0.1.0, contains an Incorrect Permission Assignment for Critical Resource vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Code execution. **CVE-2025-38743** - Dell iDRAC Service Module (iSM), version 6.0.1.0, contains a Buffer Access with Incorrect Length Value vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Code execution and Elevation of privileges. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	iDRAC Service Module version 6.0.1.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000359617/dsa-2025-311-security-update-for-dell-idrac-service-module-vulnerabilities

Affected Product	**Ubuntu**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-38350, CVE-2025-37752, CVE-2024-57996)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in the Ubuntu Linux kernel. **CVE-2025-38350** - net/sched: Always pass notifications when child class becomes empty Certain classful qdiscs may invoke their classes' dequeue handler on an enqueue operation. This may unexpectedly empty the child qdisc and thus make an in-flight class passive via qlen_notify(). Most qdiscs do not expect such behaviour at this point in time and may re-activate the class eventually anyways which will lead to a use-after-free. **CVE-2025-37752** - net_sched: sch_sfq: move the limit validation It is not sufficient to directly validate the limit on the data that the user passes as it can be updated based on how the other parameters are changed. Move the check at the end of the configuration update process to also catch scenarios where the limit is indirectly updated. **CVE-2024-57996** - net_sched: sch_sfq: don't allow 1 packet limit The current implementation does not work correctly with a limit of 1. iproute2 actually checks for this and this patch adds the check in kernel as well. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 20.04 Ubuntu 18.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-7754-1

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.