June 10, 2024

Overall Rating - High

BRITISH COLUMBIA

This notification is intended as an informational bulletin for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware that Red Hat published security advisories to address vulnerabilities in multiple products. Included were updates to address vulnerabilities in the Linux kernel for the following products:

- Red Hat CodeReady Linux Builder – multiple versions and platforms
- Red Hat Enterprise Linux – multiple versions and platforms
- Red Hat Enterprise Linux Server – multiple versions and platforms

Technical Details

In the Linux kernel, the following vulnerability has been resolved: USB: core: Fix deadlock in usb_deauthorize_interface() Among the attribute file callback routines in drivers/usb/core/sysfs.c, the interface_authorized_store() function is the only one which acquires a device lock on an ancestor device: It calls usb_deauthorize_interface(), which locks the interface's parent USB device. The will lead to deadlock if another process already owns that lock and tries to remove the interface, whether through a configuration change or because the device has been disconnected. As part of the removal procedure, device_del() waits for all ongoing sysfs attribute callbacks to complete. But usb_deauthorize_interface() can't complete until the device lock has been released, and the lock won't be released until the removal has finished. The mechanism provided by sysfs to prevent this kind of deadlock is to use the sysfs_break_active_protection() function, which tells sysfs not to wait for the attribute callback. Reported-and-tested by: Yue Sun <samsun1006219@gmail.com> Reported by: xingwei lee <xrivendell7@gmail.com>
These vulnerabilities are rated as an overall **High** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- *Ensure mitigation is performed at your next change window.*

Please notify VRM with any questions or concerns you may have.

References

- CVE-2023-6240 CVE-2024-0340 CVE-2024-26603 CVE-2019-25162 CVE-2020-36777 CVE-2023-52477 CVE-2024-26615 CVE-2023-52578 CVE-2023-52528 CVE-2023-52610 CVE-2024-26643 CVE-2024-26642 CVE-2024-26659 CVE-2024-26779 CVE-2024-26744 CVE-2024-26901 CVE-2024-26872 CVE-2024-26934 CVE-2024-26933 CVE-2024-26993 CVE-2024-27059

- Red Hat Security Advisory - RHSA-2024:3618
- Red Hat Security Advisory - RHSA-2024:3619
- Red Hat Security Advisory - RHSA-2024:3627
- Red Hat Security Advisories