November 30, 2023

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

## Technical Details

A use-after-free vulnerability in the Linux kernel's net/sched: cls_u32 component can be exploited to achieve local privilege escalation. If tcf_change_indev() fails, u32_set_parms() will immediately return an error after incrementing or decrementing the reference counter in tcf_bind_filter(). If an attacker can control the reference counter and set it to zero, they can cause the reference to be freed, leading to a use-after-free vulnerability. We recommend upgrading past commit 04c55383fa5689357bcdd2c8036725a55ed632bc.

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-2023-3609, CVE-2023-4206, CVE-2023-4207, CVE-2023-4208,
- Red Hat Security Advisory – RHSA-2023:7539
- Red Hat Security Advisory – RHSA-2023:7549
- Red Hat Security Advisory – RHSA-2023:7557
- Red Hat Security Advisories

***Please note that we will be transitioning to a new site on August 31, 2023, where we will post the vulnerability reports.***

You will be able to find all the reports that we have published as well as all future reports here: Cybersecurity Alerts