January 22, 2024

Overall Rating - High

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:

- Red Hat Enterprise Linux Server – versions AUS 7.6 x86_64 and AUS 7.7 x86_64
-

Exploitation of this vulnerability could result in a denial of service or execution of arbitrary code.

Technical Details

The kernel packages contain the Linux kernel, the core of any Linux operating system.
Security Fix(es):

- kernel: net/sched: sch_qfq component can be exploited if in qfq_change_agg function happens qfq_enqueue overhead (CVE-2023-3611)
- kernel: net/sched: Use-after-free vulnerabilities in the net/sched classifiers: cls_fw, cls_u32 and cls_route (CVE-2023-4128, CVE-2023-4206, CVE-2023-4207, CVE-2023-4208)

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-2023-3611, CVE-2023-4206, CVE-2023-4207, CVE-2023-4208
- Red Hat Security Advisory – RHSA-2024:0261
- Red Hat Security Advisory – RHSA-2024:0262
- Red Hat Security Advisories