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 of multiple vulnerabilities recently disclosed in the Linux kernel.

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. It is recommended to upgrade past commit 04c55383fa5689357bcdd2c8036725a55ed632bc.

- A use-after-free vulnerability in the Linux kernel's netfilter: nf_tables component can be exploited to achieve local privilege escalation. Flaw in the error handling of bound chains causes a use-after-free in the abort path of NFT_MSG_NEWRULE. The vulnerability requires CAP_NET_ADMIN to be triggered. It is recommended to upgrade past commit 4bedf9eee016286c835e3d8fa981ddece5338795.

- An out-of-bounds write vulnerability in the Linux kernel's net/sched: sch_qfq component can be exploited to achieve local privilege escalation. The qfq_change_agg() function in net/sched/sch_qfq.c allows an out-of-bounds write because lmax is updated according to packet sizes without bounds checks. It is recommended to upgrade past commit 3e337087c3b5805fe0b8a46ba622a962880b5d64.

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-2023-3610, CVE-2023-3611
- https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit?id=04c55383fa5689357bcdd2c8036725a55ed632bc
- https://kernel.dance/04c55383fa5689357bcdd2c8036725a55ed632bc

- https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit?id=4bedf9eee016286c835e3d8fa981ddece5338795
- https://kernel.dance/4bedf9eee016286c835e3d8fa981ddece5338795
- https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=3e337087c3b5805fe0b8a46ba622a962880b5d64
- https://kernel.dance/3e337087c3b5805fe0b8a46ba622a962880b5d64