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 a use-after-free vulnerability was found in the Linux kernel's netfilter subsystem in net/netfilter/nf_tables_api.c.

Technical Details

Mishandled error handling with NFT_MSG_NEWRULE makes it possible to use a dangling pointer in the same transaction causing a use-after-free vulnerability. This flaw allows a local attacker with user access to cause a privilege escalation issue.

It is recommended upgrading past commit 1240eb93f0616b21c675416516ff3d74798fdc97.

This vulnerability is rated as a **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-2023-3390
- https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux.git/commit/?id=1240eb93f0616b21c675416516ff3d74798fdc97
- https://kernel.dance/1240eb93f0616b21c675416516ff3d74798fdc97
- https://www.debian.org/security/2023/dsa-5448
- https://www.debian.org/security/2023/dsa-5461