BRITISH COLUMBIA

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

Summary

The Vulnerability and Risk Management (VRM) Team is aware an array indexing vulnerability was found in the netfilter subsystem of the Linux kernel.

Technical Details

A missing macro could lead to a miscalculation of the `h->nets` array offset, providing attackers with the primitive to arbitrarily increment/decrement a memory buffer out-of-bound. This issue may allow a local user to crash the system or potentially escalate their privileges on the system.

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-2023-42753
- https://access.redhat.com/security/cve/CVE-2023-42753
- https://bugzilla.redhat.com/show_bug.cgi?id=2239843
- https://www.openwall.com/lists/oss-security/2023/09/22/10