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 a use-after-free flaw was found in net/sched/cls_fw.c in classifiers (cls_fw, cls_u32, and cls_route) in the Linux Kernel.

Technical Details
This flaw allows a local attacker to perform a local privilege escalation due to incorrect handling of the existing filter, leading to a kernel information leak issue.

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-2023-4128
- https://access.redhat.com/security/cve/CVE-2023-4128
- https://bugzilla.redhat.com/show_bug.cgi?id=2225511
- https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/344H6HO6SSC4KT7PDFXSDIXKMKHISSGF/
- https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/3TYLSJ2SAI7RF56ZLQ5CQWCJLVJSD73Q/
- https://lore.kernel.org/netdev/193d6cdf-d6c9-f9be-c36a-b2a7551d5fb6@mojatatu.com/