**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 heap out-of-bounds write vulnerability in the Linux Kernel ipvlan network driver can be exploited to achieve local privilege escalation.

## Technical Details

The out-of-bounds write is caused by missing skb->cb initialization in the ipvlan network driver. The vulnerability is reachable if CONFIG_IPVLAN is enabled. It is recommended to upgrade past commit 90cbed5247439a966b645b34eb0a2e037836ea8e.

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-2023-3090
- https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=90cbed5247439a966b645b34eb0a2e037836ea8e
- https://kernel.dance/90cbed5247439a966b645b34eb0a2e037836ea8e