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 vulnerability exists in the memory management subsystem of the Linux kernel.

Technical Details

The lock handling for accessing and updating virtual memory areas (VMAs) is incorrect, leading to use-after-free problems. This issue can be successfully exploited to execute arbitrary kernel code, escalate containers, and gain root privileges.

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-2023-3269
- http://seclists.org/fulldisclosure/2023/Jul/43
- http://www.openwall.com/lists/oss-security/2023/07/28/1
- http://www.openwall.com/lists/oss-security/2023/08/25/1
- https://access.redhat.com/security/cve/CVE-2023-3269
- https://bugzilla.redhat.com/show_bug.cgi?id=2215268
- https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/U6AAA64CUPSMBW6XDTXPQJ3KQWYQ4K7L/
- https://www.openwall.com/lists/oss-security/2023/07/05/1