BRITISH COLUMBIA

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

Summary

The Vulnerability and Risk Management (VRM) Team is aware an issue was discovered in the Linux kernel before 6.3.4. ksmbd has an out-of-bounds read in smb2_find_context_vals when create_context's name_len is larger than the tag length.

Technical Details

See links below for full details.

This vulnerability is rated as a **Critical** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- Ensure mitigation is performed as soon as possible.

Please notify VRM with any questions or concerns you may have.

References

- CVE-2023-38426
- https://cdn.kernel.org/pub/linux/kernel/v6.x/ChangeLog-6.3.4
- https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/fs/ksmbd?id=02f76c401d17e409ed45bf7887148fcc22c93c85