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 kdc/do_tgs_req.c in MIT Kerberos 5 (aka krb5) 1.21 before 1.21.2 has a double free vulnerability.

Technical Details

An authenticated attacker can cause a KDC to free the same pointer twice if it can induce a failure in authorization data handling.

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-2023-39975
- https://github.com/krb5/krb5/commit/88a1701b423c13991a8064feeb26952d3641d840
- https://web.mit.edu/kerberos/www/advisories/
- https://github.com/krb5/krb5/compare/krb5-1.21.1-final...krb5-1.21.2-final