Overall rating: Critical

BRITISH COLUMBIA

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

Summary

The Vulnerability and Risk Management (VRM) Team is aware an information disclosure vulnerability exists in curl < v8.1.0 when doing HTTP(S) transfers.

Technical Details

libcurl might erroneously use the read callback (`CURLOPT_READFUNCTION`) to ask for data to send, even when the `CURLOPT_POSTFIELDS` option has been set if the same handle previously was used to issue a `PUT` request which used that callback. This flaw may surprise the application and cause it to misbehave and either send off the wrong data or use memory after free or similar in the second transfer. The problem exists in the logic for a reused handle when it is (expected to be) changed from a PUT to a POST.

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-2023-28322
- https://hackerone.com/reports/1954658
- https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/F4I75RDGX5ULSSCBE5BF3P5I5SFO7ULQ/
- https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/Z2LIWHWKOVH24COGGBCVOWDXXIUPKOMK/