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 the llhttp parser in the http module in Node v20.2.0 does not strictly use the CRLF sequence to delimit HTTP requests. This can lead to HTTP Request Smuggling (HRS). This impacts all Node.js active versions: v16, v18, and v20.

Technical Details

The CR character (without LF) is sufficient to delimit HTTP header fields in the llhttp parser. According to RFC7230 section 3, only the CRLF sequence should delimit each header-field.

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-2023-30589
- https://hackerone.com/reports/2001873