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 with a specially crafted WebP lossless file, libwebp may write data out of bounds to the heap.

Technical Details

The ReadHuffmanCodes() function allocates the HuffmanCode buffer with a size that comes from an array of precomputed sizes: kTableSize. The color_cache_bits value defines which size to use. The kTableSize array only takes into account sizes for 8-bit first-level table lookups but not second-level table lookups. libwebp allows codes that are up to 15-bit (MAX_ALLOWED_CODE_LENGTH). When BuildHuffmanTable() attempts to fill the second-level tables it may write data out-of-bounds.
The OOB write to the undersized array happens in ReplicateValue.

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-2023-5129
- https://chromium.googlesource.com/webm/libwebp/+/2af26267cdfcb63a88e5c74a85927a12d6ca1d76
- https://chromium.googlesource.com/webm/libwebp/+/902bc9190331343b2017211debcec8d2ab87e17a