September 28, 2023

Overall Rating - High

BRITISH COLUMBIA

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

Summary

On September 25, 2023, Google published a security update to address a vulnerability in the following product:

- libwebp – version 0.5.0 to versions prior to 1.3.2

Google has indicated that (CVE-2023-5129 Rejected) CVE-2023-4863, CVE-2023-41064 has an available exploit.

Technical Details

The decision to tag it as a Chrome bug caused confusion within the cybersecurity community, prompting questions regarding Google's choice to categorize it as a Google Chrome issue rather than identifying it as a flaw in libwebp.

Security consulting firm founder Ben Hawkes (who previously led Google's Project Zero team) also linked CVE-2023-4863 to the CVE-2023-41064 vulnerability addressed by Apple on September 7 and abused as part of a zero-click iMessage exploit chain (dubbed BLASTPASS) to infect fully patched iPhones with NSO Group's Pegasus commercial spyware.

These vulnerabilities are rated as an overall **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-2023-4863, CVE-2023-41064, (CVE - CVE-2023-5129 Rejected)
- BleepingComputer - Google assigns new maximum rated CVE to libwebp bug exploited in attacks.

Please note that we will be transitioning to a new site on August 31, 2023, where we will post the vulnerability reports.

You will be able to find all the reports that we have published as well as all future reports here: Cybersecurity Alerts