libwebp Supply-Chain Vulnerability

September 28, 2023

Executive Summary

Earlier in September, a Google Chrome vulnerability was originally tracked as CVE-2023-4863. The vulnerability was a heap buffer overflow in Google Chrome's WebP image library (libwebp libwebp). It has since come to light that there is a supply-chain vulnerability in the open-source libwebp library which is used in many common web browsers and applications. As the libwebp vulnerability is no longer specific to Google Chrome, it was temporarily tracked as CVE-2023-5129 with a CVSS score of 10/10. Researchers believe the same libwebp vulnerability was leveraged by NSO Group's BLASTPASS CVE-2023-41064 exploit.

Impact

Researchers have identified that there are over 700 applications that rely on libwebp and approximately 150 of them are running vulnerable versions across Windows, Linux, Apple, and Android. Many of the more common applications have already been patched, including Google Chrome, Mozilla Firefox, Brave Browser, Microsoft Edge, TOR Browser, and Opera Browser. However, this opens the doors for other applications that may be running a vulnerable libwebp to be weaponized, potentially including major applications like Discord, Keybase, Signal, Slack and Skype. While the full extent of impact is unknown it's confirmed that all native browser applications on Android are impacted.

Recommendations

We recommend updating/upgrading applications that have had patches released. Due to this vulnerability being in an underlying library, patches will be dependent on the individually impacted application developers releasing patches for their application. SRA will continue to monitor the situation and provide updates as more information becomes available.

References

- nvd.nist.gov/vuln/detail/CVE-2023-4863
- nvd.nist.gov/vuln/detail/CVE-2023-5129
- nvd.nist.gov/vuln/detail/CVE-2023-41064
- support.apple.com/en-us/HT213905
- chromereleases.googleblog.com/2023/09/stable-channel-update-for-desktop_11.html
- mozilla.org/en-US/security/advisories/mfsa2023-40
- cisa.gov/news-events/alerts/2023/09/13/mozilla-releases-security-updates-multiple-products
- citizenlab.ca/2023/09/blastpass-nso-group-iphone-zero-click-zero-day-exploit-captured-in-the-wild

- infosec.town/notes/9k5swp89shc4t888
- docs.google.com/spreadsheets/d/1QLLFYCO0FMAu1ob6mnYCapW8dnx-HXunbf_zc9QLXlM
- therecord.media/libwebp-vulnerability-more-widespread-than-expected
- tenable.com/blog/cve-2023-41064-cve-2023-4863-cve-2023-5129-faq-imageio-webp-zero-days