# Google quietly corrects previously submitted disclosure for critical webp 0-day



Getty Images

## reader comments

31 with

Google has quietly resubmitted a disclosure of a critical code-execution vulnerability affecting thousands of individual apps and software frameworks after its previous submission left readers with the mistaken impression that the threat affected only the Chrome browser.

The vulnerability originates in the libwebp code library, which Google created in 2010 for rendering images in webp, a then-new format that resulted in files that were up to 26

percent smaller than PNG images. Libwebp is incorporated into just about every app, operating system, or other code library that renders webp images, most notably the Electron framework used in Chrome and many other apps that run on both desktop and mobile devices.

Two weeks ago, Google issued a security advisory for what it said was a heap buffer overflow in WebP in Chrome. Google's formal description, tracked as CVE-2023-4863, scoped the affected vendor as "Google" and the software affected as "Chrome," even though any code that used libwebp was vulnerable. Critics warned that Google's failure to note that thousands of other pieces of code were also vulnerable would result in unnecessary delays in patching the vulnerability, which allows attackers to execute malicious code when users do nothing more than view a booby-trapped webp image.




On Monday, Google submitted a new disclosure that's tracked as CVE-2023-5129. The new entry correctly lists libwebp as the affected vendor and affected software. It also bumps up the severity rating of the vulnerability, from 8.8 out of a possible 10 to 10.

Advertisement




The lack of completeness in the first CVE Google assigned goes

well beyond being a mere academic failing. More than two weeks after the vulnerability came to light, a host of software remains unpatched. The most glaring example is Microsoft Teams.

The vulnerability description in Google's new submission provides considerably more detail. The description in the old submission was:

> *Heap buffer overflow in WebP in Google Chrome prior to 116.0.5845.187 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: Critical)*

The new description is:

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

Whether it's tracked as CVE-2023-4863 or CVE-2023-5129, the vulnerability in the libwebp is serious. Before using apps, users should ensure that the versions of Electron they use are v22.3.24, v24.8.3, or v25.8.1.

https://arstechnica.com/?p=1971345