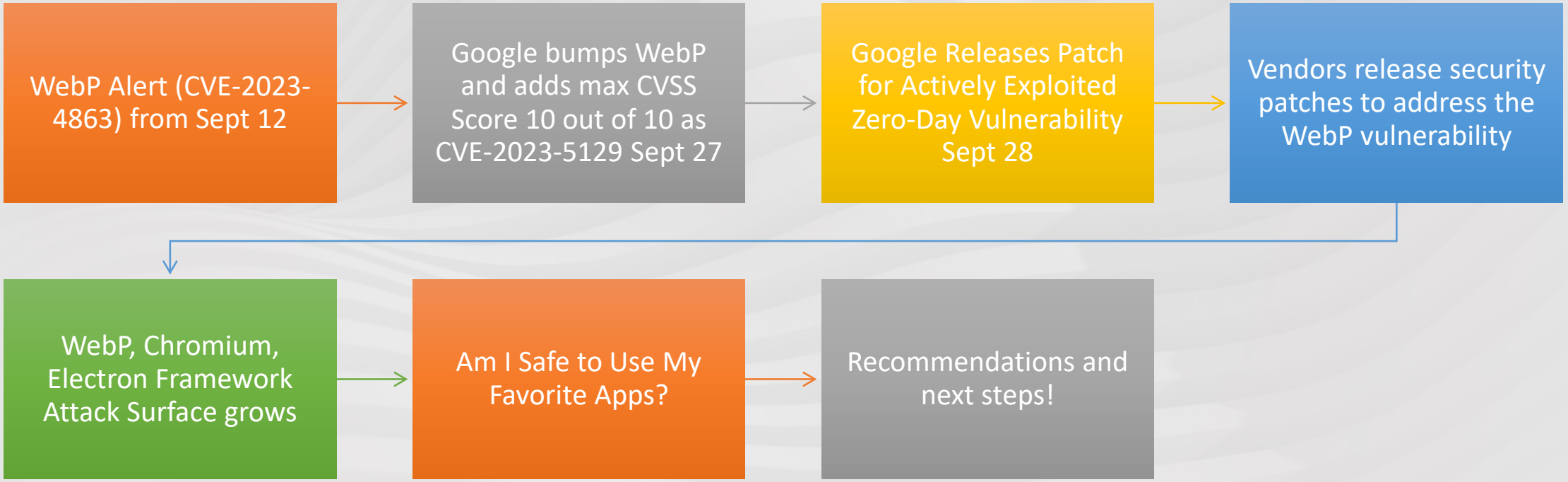
vCISO Threat Intelligence Report

Cyber Radar Alert “WebP” 9-28-2023

Contents and Timeline



Riskigy

WebP Alert (CVE-2023-4863) from Sept 12

Zero-Day Vulnerabilities in Open-source WebP (libwebp) code library are Actively being Exploited (CVE-2023-4863)

- **Mozilla patches Firefox, Thunderbird against zero-day exploited in attacks.**
  Mozilla released emergency security updates (9/12) to fix a critical zero-day vulnerability exploited in the wild, impacting its Firefox web browser and Thunderbird email client.

Recommendation on 9/12: Users are strongly advised to install updated versions of Firefox and Thunderbird to safeguard their systems against potential attacks.

- **Google fixes another Chrome zero-day bug exploited in attacks.** The critical zero-day vulnerability (CVE-2023-4863) is caused by a WebP code library (libwebp) heap buffer overflow weakness whose impact ranges from crashes to arbitrary code execution.

Recommendation on 9/12: Chrome users are advised to upgrade their web browser to version 116.0.5845.187 (Mac and Linux) and 116.0.5845.187/.188 (Windows) as soon as possible, as it patches the CVE-2023-4863 vulnerability on Windows, Mac, and Linux systems.

https://www.bleepingcomputer.com/news/security/mozilla-patches-firefox-thunderbird-against-zero-day-exploited-in-attacks/

Riskigy

New CVSS Score 10 out of 10 for CVE-2023-5129

Critical libwebp Vulnerability Under Active Exploitation - Gets Maximum CVSS Score (Sept 27)

Google has assigned a new CVE identifier for a critical security flaw in the libwebp "WebP" image library for rendering images in the WebP format that has come under active exploitation in the wild.

Now Tracked as CVE-2023-5129, the issue has been given the **maximum severity score of 10.0 on the CVSS** rating system. It has been described as an issue rooted in the Huffman coding algorithm.

Google Recommendation: Users are strongly advised to install updates – The latest as of 9/28 is Version 117.0.5938.92

.

https://thehackernews.com/2023/09/new-libwebp-vulnerability-under-active.html

Riskigy

Google Releases Patch for Actively Exploited Zero-Day

Update Chrome Now: Google Releases Patch for Actively Exploited Zero-Day Vulnerability (September 28)

Tracked as CVE-2023-5217, the high-severity vulnerability has been described as a heap-based buffer overflow in the VP8 compression format in libvpx, a free software video codec library from Google and the Alliance for Open Media (AOMedia).

The development comes as **Google assigned a new CVE identifier, CVE-2023-5129**, to the critical flaw in the libwebp image library – **originally tracked as CVE-2023-4863** – that has come under active exploitation in the wild, considering its broad attack surface.

Users are recommended to upgrade to Chrome version 117.0.5938.132 for Windows, macOS, and Linux to mitigate potential threats. Users of Chromium-based browsers such as Microsoft Edge, Brave, Opera, and Vivaldi are also advised to apply the fixes as and when they become available.

https://thehackernews.com/2023/09/update-chrome-now-google-releases-patch.html

Riskigy

Vendors release security patches to address the WebP vulnerability

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.

Many affected vendors have released security patches to address the vulnerability, including:

- 1password
- Signal
- Brave Browser
- Tor Browser
- Opera
- Bitwarden
- LibreOffice
- Suse
- Ubuntu
- LosslessCut
- Vivaldi
- NixOS
- RedHat
- Telegram
- Slack

https://arstechnica.com/security/2023/09/google-quietly-corrects-previously-submitted-disclosure-for-critical-webp-0-day/

Riskigy

WebP, Chromium, Electron Framework Attack Surface

Because CVE-2023-4863 (Original ID) and CVE-2023-5129 (New ID) was wrongly scoped as a browser vulnerability, **most scanners will fail to detect it in cases where the libwebp library is being used as a dependency**. Organizations should consider adopting alternative tooling to ensure all instances are detected and can be addressed promptly.

- ❑ **The scope of this vulnerability is much wider than initially assumed**, affecting millions of different applications worldwide.

- ❑ **Vulnerability scanners will not necessarily provide a reliable indication of the presence of this vulnerability**, due to being wrongly scoped as a Chrome issue.

https://www.rezilion.com/blog/rezilion-researchers-uncover-new-details-on-severity-of-google-chrome-zero-day-vulnerability-cve-2023-4863/

Riskigy

Am I Safe to Use My Favorite Apps?

Unfortunately, WebP vulnerability also affects an unknown number of apps. Firstly, any software using the libwebp library is affected by this vulnerability, which means each provider will need to release their own security patches.

Google launched WebP in 2010 as a solution to rendering images faster in browsers and other applications. The WebP library is utilized everywhere!

- ❑ The vulnerability is baked into many popular frameworks used to build apps.
- ❑ Google, Mozilla (FireFox), Microsoft, Brave, and Tor have all released security patches.
- ❑ Other known affected apps include Microsoft Teams, Slack, Skype, Discord, Telegram, 1Password, Signal, LibreOffice, and the Affinity suite—among many more.
- ❑ It's difficult for the average user to know which apps are affected and which ones have addressed the issue.

Riskigy

Actual Attack Surface

WebP, Chromium, Electron Framework Attack Surface cont..

While the vulnerability initially seems to target Chromium-based applications, now that we know better, we understand that it possesses the **potential to affect a much wider range of software and applications relying on the ubiquitous libwebp package for WebP codec functionality.**

Recommendations:

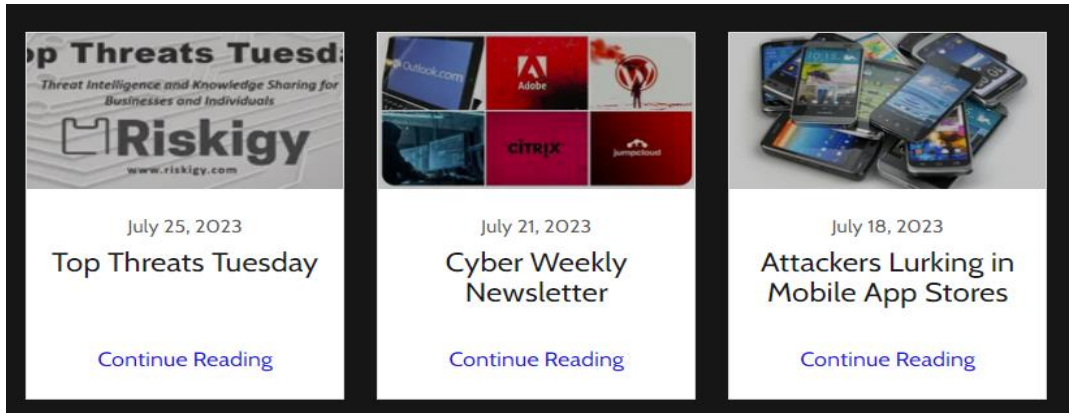
- ✓ Check the latest release versions for every app you can and look for specific references to the CVE-2023-4863 (Original ID) and CVE-2023-5129 (New ID).
- ✓ As a user or organization, the best thing you can do about the WebP vulnerability is update everything. Start with every browser you use, and then work your way through your most important apps.
- ✓ Tune vulnerability scanners and SBOM monitoring services to identify WebP vulnerabilities within your organizations systems.
- ✓ Contact critical third-party service providers for information on their WebP remediation efforts and risk.

Riskigy

Connect with Us and Get Social with the Riskigy Team

Teamwork makes the dream work! There is strength in numbers! Together we stand and the countless other reasons to connect with us!

Information & Intelligence Sharing – e: soc@riskigy.team
Mike Marrano - e: mike@riskigy.team
LinkedIn: https://www.linkedin.com/company/riskigy
Twitter: twitter.com/riskigy
Newsletter & Alerts: https://riskigy.com/blog



Riskigy