CERT-EU

Security Advisory 2023-063

Google Chrome Critical Vulnerability

September 28, 2023 — v1.2

TLP:CLEAR

History:

- *12/09/2023 — v1.0 – Initial publication*
- *15/09/2023 — v1.1 – Additional information related to impacted browsers*
- *28/09/2023 — v1.2 – New information regarding the new critical vulnerability CVE-2023-5217*

Summary

Google has released an emergency security update to address a critical vulnerability found in Chrome. This vulnerability, tracked as CVE-2023-4863, is caused by a WebP heap buffer overflow weakness. It affects Chrome running on Windows, Mac, and Linux systems and has already been exploited in the wild according to Google. Users are advised to update their Chrome web browser to version 116.0.5845.187 (Mac and Linux) and 116.0.5845.187/.188 (Windows) immediately.

Contrary to earlier reports, this critical vulnerability affects not just web browsers but also a wide range of applications that utilise the `libwebp` library for rendering WebP images. This includes Electron-based applications like Signal, 1Password, and software like Honeyview.

[Update] On September 27, Google has released another emergency security update to address a critical vulnerability found in Chrome. The vulnerability is tracked as CVE-2023-5217. Moreover, Google is aware that an exploit for CVE-2023-5217 exists in the wild.

Technical Details

The vulnerability CVE-2023-4863 is due to a heap buffer overflow in the WebP image format library. This flaw allows for arbitrary code execution or can cause the application to crash. It was discovered and reported by Apple Security Engineering and Architecture (SEAR) and The Citizen Lab at The University of Toronto's Munk School. The CVSS score for other related vulnerabilities is between 8.8 and 9.6, indicating a critical level of severity.

[Update] The high-severity zero-day vulnerability CVE-2023-5217 is caused by a heap buffer overflow weakness in the VP8 encoding of the open-source `libvpx` video codec library, a flaw whose impact ranges from app crashes to arbitrary code execution. In addition, other Chromium related projects could be vulnerable if they depend on the library.

Affected Products

- CVE-2023-4863:
  - Google Chrome version prior to 116.0.5845.187/.188
  - Chromium-based browsers like Microsoft Edge, Brave, Opera, and Vivaldi that have not yet applied the fix
  - Other software using the `libwebp` library, including Honeyview, Affinity, Gimp, Inkscape, LibreOffice, Telegram, ffmpeg, and various Android and cross-platform apps built with Flutter, as well as Firefox products as specified in SA2023-066.
- **[Update]** CVE-2023-5217:
  - Google Chrome version prior to 117.0.5938.132
  - Other Chromium related projects depending on the `libvpx` library.

Recommendations

Update the affected products to the latest versions available as soon as possible to mitigate the vulnerabilities.

References

[1] https://www.google.com/chrome/security/

[2] https://www.bleepingcomputer.com/

[3] https://www.mozilla.org/en-US/security/advisories/mfsa2023-40/

[4] https://learn.microsoft.com/en-us/deployedge/microsoft-edge-relnotes-security#september-12-2023

[5] https://chromereleases.googleblog.com/2023/09/stable-channel-update-for-desktop_27.html