CERT-EU

Security Advisory 2023-093

High Vulnerabilities in Google Chrome

November 29, 2023 — v1.0

TLP:CLEAR

History:

- *29/11/2023 — v1.0 – Initial publication*

Summary

On November 28, Google has released an emergency security update to address six high vulnerabilities found in Chrome. Google is aware that an exploit exists for one of the vulnerabilities, tracked as `CVE-2023-6345` [1].

Technical Details

The high-severity zero-day vulnerability `CVE-2023-6345` is caused by an integer overflow weakness within the Skia open-source 2D graphics library, posing risks ranging from crashes to the execution of arbitrary code (Skia is also used as a graphics engine by other products like ChromeOS, Android, and Flutter) [2].

The other vulnerabilities are:

- CVE-2023-6348: Type Confusion in `Spellcheck`.
- CVE-2023-6347: Use after free in `Mojo`.
- CVE-2023-6346: Use after free in `WebAudio`.
- CVE-2023-6350: Out of bounds memory access in `libavif`.
- CVE-2023-6351: Use after free in `libavif`.

Affected Products

Google Chrome version prior to 119.0.6045.199 for Mac and Linux and prior to 119.0.6045.199/.200 for Windows are affected by these vulnerabilities. Other Chromium related projects depending on the `Skia` library might also be affected.

Recommendations

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

References

[1] https://chromereleases.googleblog.com/2023/11/stable-channel-update-for-desktop_28.html

[2] https://www.bleepingcomputer.com/news/security/google-chrome-emergency-update-fixes-6th-zero-day-exploited-in-2023/