CERT-EU

Security Advisory 2024-044

Zero-day Vulnerability in Chrome

May 16, 2024 — v1.0

TLP:CLEAR

History:

- *16/05/2024 — v1.0 – Initial publication*

Summary

On May 15, 2024, Google has released an advisory addressing nine vulnerabilities, including a new zero-day bug identified as `CVE-2024-4947`. It has been reported that this vulnerability is being actively exploited [1]. This is the seventh zero-day vulnerability fixed by Google this year.

Technical Details

- The vulnerability `CVE-2024-4947` is a type confusion bug in the V8 JavaScript and WebAssembly engine [2].
- The vulnerability `CVE-2024-4761` is an out-of-bounds write bug impacting the V8 JavaScript and WebAssembly engine [3].
- The vulnerability `CVE-2024-4671` is a use-after-free in a Visuals component [4].
- The vulnerability `CVE-2024-3159` is an out of bounds memory access in the V8 engines [5].
- The vulnerability `CVE-2024-2887` is a type confusion bug in the WebAssembly engine [6].
- The vulnerability `CVE-2024-2886` is a use after free bug in WebCodecs [6].
- The vulnerability `CVE-2024-0519` is an out of bounds memory access in the V8 engines [7].

Affected Products

Google Chrome prior to version 125.0.6422.60/.61 for Windows and Mac, 125.0.6422.60 for Linux are impacted [1]. Other Chromium-based browsers such as Microsoft Edge, Brave, Opera, and Vivaldi are also affected.

Recommendations

It is recommended updating Google Chrome browsers to the latest version. It is also advised updating other Chromium-based browsers when fixes become available.

References

[1] https://chromereleases.googleblog.com/2024/05/stable-channel-update-for-desktop_15.html

[2] https://thehackernews.com/2024/05/google-patches-yet-another-actively.html

[3] https://thehackernews.com/2024/05/new-chrome-zero-day-vulnerability-cve.html

[4] https://thehackernews.com/2024/05/chrome-zero-day-alert-update-your.html

[5] https://chromereleases.googleblog.com/2024/04/stable-channel-update-for-desktop.html

[6] https://chromereleases.googleblog.com/2024/03/stable-channel-update-for-desktop_26.html

[7] https://www.cert.europa.eu/publications/security-advisories/2024-012/