Security Advisory 2023-024

Type confusion flaw in Google Chrome

April 18, 2023 — v1.0

TLP:CLEAR

History:

• 18/04/2023 — v1.0 – Initial publication

Summary

Google has released out-of-band updates to address a vulnerability in its Chrome web browser, identified as CVE-2023-2033. The high-severity flaw is a type confusion issue within the V8 JavaScript engine. Users of Google Chrome, as well as other Chromium-based browsers such as Microsoft Edge, Brave, Opera, and Vivaldi, are strongly advised to update to the latest version to mitigate potential threats.

Technical Details

CVE-2023-2033 is a type confusion vulnerability in the V8 JavaScript engine used by Google Chrome and other Chromium-based web browsers. Type confusion issues can lead to a crash of the application, or code execution when a user visits a specially crafted and malicious HTML page. This vulnerability shares similarities with CVE-2022-1096, CVE-2022-1364, CVE-2022-3723, and CVE-2022-4262, which were abused type confusion flaws in V8 that were patched by Google in 2022.

Although Google acknowledged the existence of an exploit for CVE-2023-2033 in the wild, the company has not provided further technical details or indicators of compromise (IoCs) to prevent additional exploitation by threat actors.

Affected Products

The following products are affected by CVE-2023-2033:

• Google Chrome prior to version 112.0.5615.121
• Chromium-based browsers such as Microsoft Edge, Brave and Opera that have not yet applied the relevant fixes
Recommendations

To mitigate the risks associated with CVE-2023-2033, users are advised to:

- Update Google Chrome to version 112.0.5615.121 for Windows, macOS, and Linux.
- Update other Chromium-based browsers as soon as fixes become available.

References