Security Advisory 2023-035

Type Confusion Flaw in Google Chrome

June 6, 2023 — v1.0

TLP: CLEAR

History:
- 06/06/2023 — v1.0 – Initial publication

Summary

Google has released a security update to address a zero-day vulnerability in its Chrome web browser, identified as CVE-2023-3079. The high-severity flaw is a type confusion issue within the V8 JavaScript engine. Google is aware that an exploit for this vulnerability exists in the wild.

Users of Google Chrome are strongly advised to update to the latest version to mitigate potential threats.

Technical Details

CVE-2023-3079 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.

Although Google acknowledged the existence of an exploit for CVE-2023-3079 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-2023-3079:

- Google Chrome prior to version 114.0.5735.110 for Windows, and prior to version 114.0.5735.106 for Linux and Mac.
Recommendations

To mitigate the risks associated with CVE-2023-3079, users are advised to:

- Update Google Chrome to the latest version.

References