CERT-EU

Security Advisory 2023-100

High Severity Vulnerability in Google Chrome

December 22, 2023 — v1.1

TLP:CLEAR

History:

- *21/12/2023 — v1.0 – Initial publication*
- *22/12/2023 — v1.1 – Add affected products*

Summary

On December 20, 2023, Google released an advisory regarding a new high severity vulnerability in its web browser [1]. Google is aware that an exploit for this vulnerability exists in the wild.

It is recommended updating as soon as possible.

Technical Details

The vulnerability `CVE-2023-7024` is caused by a heap buffer overflow in the WebRTC component. The flaw was reported by Clément Lecigne and Vlad Stolyarov of Google's Threat Analysis Group on 2023-12-19 and fixed in just one day. The fact that the issue was discovered by Google TAG suggests it was exploited by a nation-state actor or by a surveillance firm [2]. Google has not shared further details about the vulnerability, stating that:

> Access to bug details and links may be kept restricted until a majority of users are updated with a fix. We will also retain restrictions if the bug exists in a third party library that other projects similarly depend on, but haven't yet fixed.

Affected Products

This vulnerability affects Google Chrome versions below 120.0.6099.129 for Mac, Linux, and versions below 120.0.6099.129/130 for Windows.

[UPDATE] This vulnerability also affects Chromium-based web browser such as Microsoft Edge [3], Brave, Opera, and Vivaldi.

Recommendations

It is recommended updating as soon as possible.

References

[1] https://chromereleases.googleblog.com/2023/12/stable-channel-update-for-desktop_20.html

[2] https://securityaffairs.com/156231/security/google-addressed-a-new-actively-exploited-chrome-zero-day.html

[3] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-7024