

A decorative graphic in the top right corner consisting of a white vertical bar, a blue horizontal bar, and another white vertical bar.

Newscast critical vulnerability in Google Chrome

Table of content

GOOGLE	2
Chrome - CVE-2023-7024	2
Type of vulnerability.....	2
Risks.....	2
Criticality (CVSS v3.1 base score)	2
Product impacted.....	2
Recommendations.....	2
Proof of concept.....	3
SOURCES	4

Google

On 12/20/2023, [Google](#) released an emergency update to fix an **exploited** zero-day flaw in the [Chrome](#) web browser.

Chrome - CVE-2023-7024



Security researchers Clément Lecigne and Vlad Stolyarov of the Google Threat Analysis Group (TAG) have identified a buffer overflow vulnerability in the *WebRTC* component of Google Chrome.

The exploitation of this CVE by a remote and unauthenticated attacker allows, by persuading a victim to consult a specifically forged website, to execute arbitrary code and cause a crash of the application.



The publisher mentions that the vulnerability is exploited in the wild.

Type of vulnerability

- **CWE-122**: Heap-based Buffer Overflow

Risks

- Arbitrary code execution
- Denial of service

Criticality (CVSS v3.1 base score)

Attack vector	Network	Scope	Unchanged
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	None	Impact on integrity	High
User Interaction	Required	Impact on availability	High

Product impacted

- Google Chrome versions prior to 120.0.6099.129 and 120.0.6099.130

Recommendations

It is recommended to update Google Chrome:

- To version 120.0.6099.129 for MacOS and Linux,
- To version 120.0.6099.129/130 for Windows.

Publisher's website

Additional information is available at [Google Bulletin](#).

Proof of concept

No proof of concept is available in open source.

Sources

GOOGLE

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

CVE-2023-7024

- <https://securityaffairs.com/156231/security/google-addressed-a-new-actively-exploited-chrome-zero-day.html>
- <https://exchange.xforce.ibmcloud.com/vulnerabilities/275490>
- <https://vuldb.com/?id.248580>