Security Advisory 2024-012

Vulnerability in Chrome

January 19, 2024 — v1.0

TLP:CLEAR

History:

- *19/01/2024 — v1.0 – Initial publication*

Summary

On January 16, 2024, Google has released an advisory addressing a zero-day vulnerability identified as `CVE-2024-0519`, which affects the V8 engine in Google Chromium. This vulnerability allows for out-of-bounds memory access, potentially leading to heap corruption through a crafted HTML page. It has been reported that this vulnerability is being actively exploited.

Technical Details

`CVE-2024-0519` is a critical vulnerability in the V8 JavaScript and WebAssembly engine used by Chromium-based browsers. It allows remote attackers to potentially exploit heap corruption via a crafted HTML page, leading to out-of-bounds memory access.

Affected Products

- Google Chrome prior to version 120.0.6099.234 for Mac and 120.0.6099.224 for Linux and 120.0.6099.224/225 for Windows are impacted;
- Other Chromium-based web browsers such as Microsoft Edge, Brave, Opera, and Vivaldi are possibly impacted.

Recommendations

It is recommended updating the Google Chrome browser to the latest version as it includes patches for `CVE-2024-0519` and other vulnerabilities. It is recommended to enable automatic updates for Chrome to ensure timely application of security patches.

It is also recommended keeping other Chromium-based browser up-to-date.

References

[1] https://nvd.nist.gov/vuln/detail/CVE-2024-0519

[2] https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_16.html