

Security Advisory 2024-062

Vulnerabilities in Chrome and Chromium based Browsers

June 21, 2024 — v1.0

TLP:CLEAR

History:

- *21/06/2024 — v1.0 – Initial publication*

Summary

Google has released a critical security update for its Chrome Browser, addressing six high-severity vulnerabilities that could lead to serious security issues. Chromium-based browsers are also impacted.

Technical Details

The vulnerabilities patched in this update include:

- **CVE-2024-6100:** Type confusion in V8
- **CVE-2024-6101:** Inappropriate implementation in WebAssembly
- **CVE-2024-6102:** Out-of-bounds memory access in Dawn
- **CVE-2024-6103:** Use-after-free in Dawn

Affected Products

- Google Chrome versions prior to 126.0.6478.114/115 for Windows and Mac
- Google Chrome versions prior to 126.0.6478.114 for Linux
- Chromium-based browsers

Recommendations

Users are strongly advised to update their Chromium-based browsers to the latest version available.

References

- [1] https://chromereleases.googleblog.com/2024/06/stable-channel-update-for-desktop_18.html
- [2] <https://cybersecuritynews.com/google-chrome-security-patch-2/>