Hive Pro

THREAT ADVISORY

Google fixes multiple vulnerabilities in Chrome	TA2022002
Threat Level AMBER	**Publish Date –** Jan 6, 2022

Google Chrome has been updated to version 97, which addresses 37 security flaws. Google has classed ten of them as High and one as Critical, while the remaining thirteen have been classified as Medium or Low.
These flaws pose a high risk to all Linux, macOS, and Windows users, and users should act by updating Chrome to version 97.0.4692.71.

This advisory addresses the following 24 Google-disclosed vulnerabilities. To avoid exploitation, the rest of them will be uncovered once most users have been upgraded.

- CVE-2022-0096: Use after free in Storage.
- CVE-2022-0097: Inappropriate implementation in DevTools.
- CVE-2022-0098: Use after free in Screen Capture.
- CVE-2022-0099: Use after free in Sign-in.
- CVE-2022-0100: Heap buffer overflow in Media streams API.
- CVE-2022-0101: Heap buffer overflow in Bookmarks.
- CVE-2022-0102: Type Confusion in V8 .
- CVE-2022-0103: Use after free in SwiftShader.
- CVE-2022-0104: Heap buffer overflow in ANGLE.
- CVE-2022-0105: Use after free in PDF.
- CVE-2022-0106: Use after free in Autofill.
- CVE-2022-0107: Use after free in File Manager API.
- CVE-2022-0108: Inappropriate implementation in Navigation.
- CVE-2022-0109: Inappropriate implementation in Autofill.
- CVE-2022-0110: Incorrect security UI in Autofill.
- CVE-2022-0111: Inappropriate implementation in Navigation.
- CVE-2022-0112: Incorrect security UI in Browser UI.
- CVE-2022-0113: Inappropriate implementation in Blink.
- CVE-2022-0114: Out of bounds memory access in Web Serial.
- CVE-2022-0115: Uninitialized Use in File API.
- CVE-2022-0116: Inappropriate implementation in Compositing.
- CVE-2022-0117: Policy bypass in Service Workers.
- CVE-2022-0118: Inappropriate implementation in WebShare.
- CVE-2022-0120: Inappropriate implementation in Passwords.

Vulnerability Details

CVE ID	Affected CPE	Vulnerability Name	CWE ID
CVE-2022-0096	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	Use after free in Storage.	CWE-416
CVE-2022-0097	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	Inappropriate implementation in DevTools.	

Vulnerability Details

CVE ID	Affected CPE	Vulnerability Name	CWE ID
CVE-2022-0098	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	Use after free in Screen Capture.	CWE-416
CVE-2022-0099	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	Use after free in Sign-in.	CWE-416
CVE-2022-0100	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	Heap buffer overflow in Media streams API.	CWE-122
CVE-2022-0101	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	Heap buffer overflow in Bookmarks.	CWE-122
CVE-2022-0102	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	Type Confusion in V8 .	CWE-843
CVE-2022-0103	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	Use after free in SwiftShader.	CWE-416
CVE-2022-0104	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	Heap buffer overflow in ANGLE.	CWE-122
CVE-2022-0105	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	Use after free in PDF.	CWE-416
CVE-2022-0106	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	Use after free in Autofill.	CWE-416
CVE-2022-0107	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	Use after free in File Manager API.	CWE-416
CVE-2022-0108	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	Inappropriate implementation in Navigation.	CWE-358
CVE-2022-0109	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	Inappropriate implementation in Autofill.	CWE-358
CVE-2022-0110	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	Incorrect security UI in Autofill.	CWE-451
CVE-2022-0111	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	Inappropriate implementation in Navigation.	CWE-358
CVE-2022-0112	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	Incorrect security UI in Browser UI.	CWE-451
CVE-2022-0113	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	Inappropriate implementation in Blink.	CWE-358
CVE-2022-0114	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	Out of bounds memory access in Web Serial.	CWE-119
CVE-2022-0115	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	Uninitialized Use in File API.	CWE-824, CWE-908

Hive Pro

THREAT ADVISORY

Vulnerability Details

CVE ID	Affected CPE	Vulnerability Name	CWE ID
CVE-2022-0116	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	Inappropriate implementation in Compositing.	CWE-345, CWE-358
CVE-2022-0117	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	Policy bypass in Service Workers.	CWE-285
CVE-2022-0118	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	Inappropriate implementation in WebShare.	CWE-358
CVE-2022-0120	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	Inappropriate implementation in Passwords.	CWE-358

Patch Links

https://chromereleases.googleblog.com/2022/01/stable-channel-update-for-desktop.html

References

https://www.cisa.gov/uscert/ncas/current-activity/2022/01/05/google-releases-security-updates-chrome
https://www.forbes.com/sites/gordonkelly/2022/01/05/google-chrome-hack-warning-new-attacks-exploits-upgrade-chrome-now/?sh=467db05810b0