Hive Pro

Threat Level

Green

THREAT ADVISORY

VULNERABILITY REPORT

Multiple vulnerabilities addressed by Google with Chrome 105

Date of Publication	Admiralty code	TA Number
September 1, 2022	A1	TA2022190

Summary

Google Chrome addresses multiple vulnerabilities in its latest stable channel update for Windows, Mac, and Linux.

CVEs

CVE	NAME	PATCH
CVE-2022-3038	Use after free in Network Service	✓
CVE-2022-3039	Use after free in WebSQL	✓
CVE-2022-3040	Use after free in Layout	✓
CVE-2022-3041	Use after free in WebSQL	✓
CVE-2022-3042	Use after free in PhoneHub	✓
CVE-2022-3043	Heap buffer overflow in Screen Capture	✓
CVE-2022-3044	Inappropriate implementation in Site Isolation	✓
CVE-2022-3045	Insufficient validation of untrusted input in V8	✓
CVE-2022-3046	Use after free in Browser Tag	✓
CVE-2022-3071	Use after free in Tab Strip	✓

Technical Details

Seven of the ten Chrome vulnerabilities are caused by the Use-After-Free (UAF) flaw. This is a vulnerability related to the incorrect use of dynamic memory during program operation. Successful exploitation of this the issue may lead to data corruption, program crash, or arbitrary code execution. In recent browser versions, several controls have been introduced that make exploitation of these Use-After-Free vulnerabilities much harder but despite this, they still seem to persist.

Vulnerability Details

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2022-3038	Google Chromium: 105.0.5195.0 - 105.0.5195.51	cpe:2.3:a:google:chromium:105.0.5195.-:*:*:*:*:*:*:*	CWE-416
CVE-2022-3039			CWE- 416
CVE-2022-3040			CWE-416
CVE-2022-3041			CWE-416
CVE-2022-3042			CWE-416
CVE-2022-3043			CWE-122
CVE-2022-3044			CWE-358
CVE-2022-3045			CWE-20
CVE-2022-3046			CWE-416
CVE-2022-3071			CWE-416

Patch Details

Update Google Chrome to version 105.0.5195.52
Patch Link
https://www.google.com/intl/en/chrome/?standalone=1

References

https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_30.html

What Next?

Book a free demo with **HivePro Uni5** to check your exposure to this advisory. HivePro Uni5 is a Continuous Threat Exposure Management Solution that proactively reduces an organization's attack surface before it gets exploited.

At Hive Pro we take a long hard look at your vulnerabilities so you can bolster your defenses and fine-tune your offensive cybersecurity tactics.

REPORT GENERATED ON

September 1, 2022 • 6:22 AM

More at www.hivepro.com