Hive Pro

Threat Level

Green

THREAT ADVISORY

VULNERABILITY REPORT

Stable Channel Update in Chrome for Windows, Mac and Linux

Date of Publication	Admiralty code	TA Number
13 June 2022	A1	TA2022115

Summary

A list of security fixes has been addressed in the latest version for Windows, Mac and Linux. There are seven security fixes in which four are high severity vulnerabilities (as per Chrome). These vulnerabilities involve the exploitation of vulnerable systems, access to potentially sensitive information etc.

CVEs

CVE	NAME	PATCH
CVE-2022-2007	Use-after-free	✓
CVE-2022-2008	Buffer overflow	✓
CVE-2022-2010	Out-of-bounds read	✓
CVE-2022-2011	Use-after-free	✓

Technical Details

#1 The first vulnerability which has been assigned CVE-2022-2007, allows a remote attacker to compromise the vulnerability system, the attacker creates a malicious web page and tricks the victim into visiting it which then triggers use-after-free error and executes arbitrary code on the target system. The second vulnerability CVE-2022-2008, allows the attacker to compromise the affected system by triggering a stack-based buffer overflow and execute arbitrary code.

#2 The third vulnerability tracked as CVE-2010 allows a remote attacker to gain access to sensitive information. This vulnerabilities aids the attacker in triggering an out-of-bounds read error and gain access to sensitive data. The last vulnerability CVE-2022-2011, helps the attacker successfully exploit the security flaw and compromise the vulnerable system.

#3 These vulnerabilities have been addressed and patched up in the latest version 102.0.5005 for Windows, Mac and Linux. Organizations are encouraged to mitigate the situation by updating their browsers.

Vulnerability Details

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2022-2007	Google Chrome: 90.0.4430.72 - 102.0.5005.63	cpe:2.3:a:google:google_chrome:*:*:*:*:*:*:*:*	CWE- 416
CVE-2022-2008			CWE-119
CVE-2022-2010			CWE-125
CVE-2022-2011			CWE-416

Patch Links

https://www.google.com/intl/en/chrome/?standalone=1

References

https://chromereleases.googleblog.com/2022/06/stable-channel-update-for-desktop.html

What Next?

Book a free demo with **HivePro Uni5** to check your exposure to this advisory. HivePro Uni5 is a 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

13 June 2022 • 1:45 AM

More at www.hivepro.com