Hive Pro

THREAT ADVISORY

Multiple Google Chrome Vulnerabilities affects all Platforms

TA2022065

Threat Level GREEN

Publish Date – March 18, 2022

Chrome versions prior to 99.0.4844.74 affects Windows, Mac, and Linux. Vendor has released fixes for ten vulnerabilities that allow an attacker to gain control of a vulnerable system.

Nine of the ten Chrome vulnerabilities are impacted by Use-After-Free (UAF) flaw. This is a vulnerability related to incorrect use of dynamic memory during program operation. Successful exploitation of this 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.

This update fixed 10 security vulnerabilities which have been mentioned in the table below. We recommend organizations to update to Chrome 99.0.4844.74 for Windows, Mac and Linux to avoid exploitation and mitigate any potential threats.

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2022-0971	Google Chrome prior to Chrome 99.0.4844.74	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	Use after free in Blink Layout	CWE-416
CVE-2022-0972			Use after free in Extensions	CWE-416
CVE-2022-0973			Use after free in Safe Browsing	CWE-416
CVE-2022-0974			Use after free in Splitscreen	CWE-416
CVE-2022-0975			Use after free in ANGLE	CWE-416
CVE-2022-0976			Heap buffer overflow in GPU	CWE-122
CVE-2022-0977			Use after free in Browser UI	CWE-416
CVE-2022-0978			Use after free in ANGLE	CWE-416
CVE-2022-0979			Use after free in Safe Browsing	CWE-416
CVE-2022-0980			Use after free in New Tab Page	CWE-416

Patch Link

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

References

https://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop_15.html