Hive Pro

THREAT ADVISORY

For the third month in a row, it's time to update Google Chrome

TA202144

Threat Level RED

Publish Date – Oct 31, 2021

Multiple vulnerabilities have been discovered in the world's most popular browser. Two of them have been used in the wild (CVE-2021-38000, CVE-2021-38003). Google has recently patched these vulnerabilities in Chrome version 95.0.4638.69 for Windows, Mac, and Linux.

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2021-38000	Google Chrome 95	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	Insufficient validation of untrusted input in Intents.	
CVE-2021-38003			Inappropriate implementation in V8.	
CVE-2021-37997			Use after free in Sign-In.	CWE-416
CVE-2021-37998			Use after free in Garbage Collection.	CWE-416
CVE-2021-37999			Insufficient data validation in New Tab Page.	
CVE-2021-38001			Type Confusion in V8.	CWE-843
CVE-2021-38002			Use after free in Web Transport.	CWE-416

Patch Link

https://chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop_28.html

References

https://www.zdnet.com/article/google-fixes-two-high-severity-zero-day-flaws-in-chrome/
https://thedigitalhacker.com/chrome-95-update-patches-expose-zero-day-flaws-flaws-revealed-at-tianfu-cup/