Hive Pro

THREAT ADVISORY

Chrome's eleventh zero-day vulnerability for the year 2021 has been patched

TA202138

Threat Level AMBER

Publish Date – Sept 26, 2021

A vulnerability in Chrome and Microsoft edge(Chromium based) exists as a result of a use-after-free issue when processing HTML data in Google Chrome's Portals component. A remote attacker can create a specially designed site, fool the victim into visiting it, trigger a use-after-free error, and execute arbitrary code on the machine. This vulnerability has also been exploited in the wild. Google has issued an emergency update (94.0.4606.61) addressing the problem.

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2021-37973	Google Chrome up to 93.0.4577.82, Microsoft Edge (Chromium-based) up to 93.0.961.52	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*, cpe:2.3:a:microsoft:microsoft_edge_\(chromium-based\):*:*:*:*:*:*:*:*	Use after free in Portals.	CWE-416

Patch Link

https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop_24.html

References

https://www.bleepingcomputer.com/news/security/emergency-google-chrome-update-fixes-zero-day-exploited-in-the-wild/
https://www.cybersecurity-help.cz/vdb/SB2021092428