Hive Pro

THREAT ADVISORY

Google patches chrome zero-day vulnerabilities being exploited in the wild.

TA202133

Threat Level Red

Publish Date – September 16, 2021

Google just released a major security update for Chrome that addresses eleven vulnerabilities, including two zero-day flaws that have been exploited in the wild. A remote attacker might take use of the flaws by tricking an unsuspecting victim into visiting a specially designed website they generated, which would cause a type confusion error, allowing them to run arbitrary code on the affected system. Users are advised to update their browsers to the latest version (91.0.4472.164) as soon as practicable.

Vulnerability Details

CVE ID	Affected CPEs	Vulnerability Name
CVE-2021-30632	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	Out of bounds write in V8 JavaScript Engine
CVE-2021-30633	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	Use after free in the Indexed DB API.
CVE-2021-30625	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	Use after free in Selection API
CVE-2021-30626	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	Out of bounds memory access in ANGLE
CVE-2021-30627	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	Type Confusion in Blink layout
CVE-2021-30628	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	Stack buffer overflow in ANGLE
CVE-2021-30629	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	Use after free in Permissions
CVE-2021-30630	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	Inappropriate implementation in Blink
CVE-2021-30631	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	Type Confusion in Blink layout

References

https://threatpost.com/google-chrome-zero-day-exploited/169442/
https://www.securitymagazine.com/articles/96096-google-patches-chrome-zero-day-exploited-in-the-wild