



**Bulletin**: 2021-005

Date: 06/11/2021

Name: Chrome/IE 0 Days

Classification: Browser Zero Days

## **Summary**

Google issued multiple <u>patches</u> for 14 browser vulnerabilities, out of which one is confirmed to be exploited in the wild. Google has not yet published additional details or IOCs in this specific attack.

For Patch Tuesday, Microsoft has issued <u>patches</u> for six vulnerabilities targeting the Windows Environment. <u>One</u> of these is a zero day vulnerability flaw that allows remote code execution in a Windows HTML component, which is within the context of the Trident Browser Engine,

## **Technical Details**

## Infection Vector

The browser zero days are primarily affecting Chrome/IE browsers, however, since Microsoft Edge is also now based on Chrome, Edge users will also be vulnerable to these flaws. Below is a table, listing all the HIGH severity vulnerabilities, with associated CVEs patched by Google.

CVE	Severity	Browsers Description	In the wild exploitation
CVE-2021-33742	High	Internet Explorer Windows MSHTML Platform Remote	Yes. Confirmed by Google Threat Analysis Group.
		Code Execution	





www.menlosecurity.com





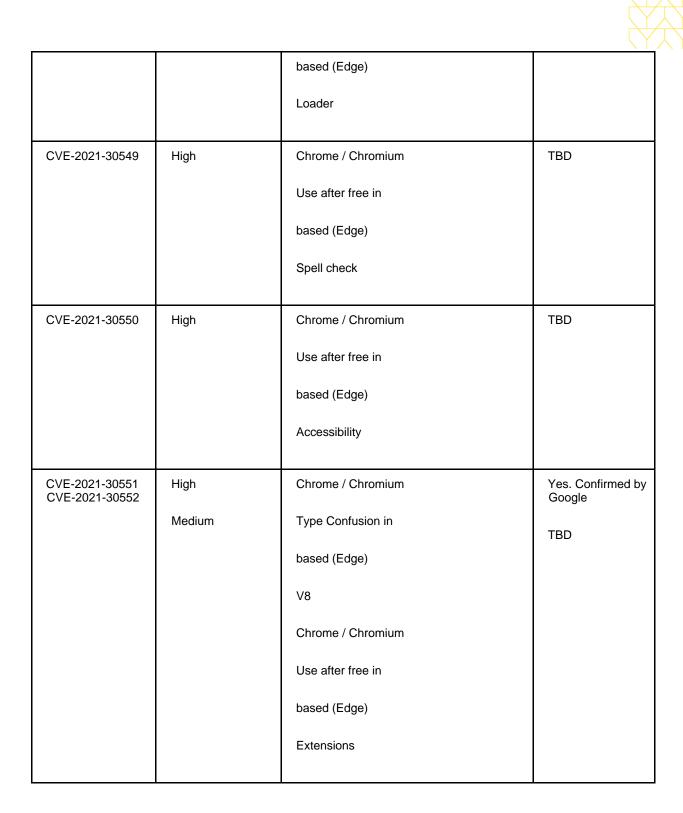


CVE-2021-30544	Critical	Chrome / Chromium	TBD
		Use after free in	
		based (Edge)	
		BFCache	
CVE-2021-30545	High	Chrome / Chromium	TBD
	· ·		
		Use after free in	
		based (Edge)	
		Extensions	
2)/=			
CVE-2021-30546	High	Chrome / Chromium	TBD
		Use after free in	
		Based (Edge)	
		Dased (Luge)	
		Autofill	
CVE-2021-30547	High	Chrome / Chromium	TBD
		Out of bounds write	
		Cut of Bournas write	
		based (Edge)	
		in ANGLE	
CVE-2021-30548	High	Chrome / Chromium	TBD
		Use after free in	











CVE-2021-30553 Medium Chrome / Chromium based (Edge)

## Protection

Use after free in Network service -TBD

Customers using the Menlo Cloud Security Platform are protected against such vulnerabilities by design! With Menlo, when a user visits a website via the isolation platform, all active content is executed in the Menlo Isolation Cloud, which means that any malicious JavaScript executes in an isolated browser, running in Menlo's cloud-based isolation platform - Not on the users device. Menlo protects all devices—including mobile.

Menlo labs is actively monitoring for any IOCs and will update the platform, once additional details about the threat are available.

© 2021 Menlo Security Inc. All rights reserved.