MENLO SECURITY

1 650.614.1705 ☎
support@menlosecurity.com ✉
www.menlosecurity.com

Menlo labs.

Bulletin: 2021-005

Date: 06/11/2021

Name: Chrome/IE 0 Days

Classification: Browser Zero Days

Summary

Google issued multiple patches 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 patches for six vulnerabilities targeting the Windows Environment. One 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 Code Execution	Yes. Confirmed by Google Threat Analysis Group.

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

		based (Edge) Loader	
CVE-2021-30549	High	Chrome / Chromium Use after free in based (Edge) Spell check	TBD
CVE-2021-30550	High	Chrome / Chromium Use after free in based (Edge) Accessibility	TBD
CVE-2021-30551 CVE-2021-30552	High Medium	Chrome / Chromium Type Confusion in based (Edge) V8 Chrome / Chromium Use after free in based (Edge) Extensions	Yes. Confirmed by Google TBD

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.