

# Google Chrome Hit by Third Zero-Day Vulnerability Attack

Severity: High

Date: 06<sup>th</sup> May 2023

## Description

Google Chrome prior to 114.0.5735.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

## Impact

CVE-2023-3079 is a vulnerability that stems from a type of confusion in the V8 JavaScript engine and has been uncovered by Google's Threat Analysis Group (TAG), a "task-force" dedicated to protecting users from state-sponsored malware attacks and other advanced persistent threats.

"Google is aware that an exploit for CVE-2023-3079 exists in the wild," the Chrome team says.

As per usual, Google is refraining from revealing bug details "until a majority of users are updated with a fix."

## Fix

To address this critical issue, users are advised to upgrade their Google Chrome browser to the latest version. The recommended updates include version 114.0.5735.110 for Windows and version 114.0.5735.106 for macOS and Linux. Chromium-based browsers – Opera, Brave, Microsoft Edge, etc. – will also require patching.

These latest versions also include fixes for bugs unearthed by Google via internal audits, fuzzing and through other initiatives.

## Reference Links

<https://www.bleepingcomputer.com/news/security/google-fixes-new-chrome-zero-day-flaw-with-exploit-in-the-wild/>