



**THREAT ADVISORY**



**VULNERABILITY  
REPORT**

**Google addresses new vulnerabilities in Chrome**

Date of Publication

June 23, 2022

Admiralty code

A1

TA Number

TA2022132

# Summary

Google Chrome addresses nine vulnerabilities in its latest stable channel update for Windows, Mac and Linux

## ⚙️ CVEs

CVE	NAME	PATCH
CVE-2022-2156	Use after free in Base	✓
CVE-2022-2157	Use after free in interest groups	✓
CVE-2022-2158	Type confusion un V8	✓
CVE-2022-2160	Insufficient policy enforcement in Devtools	✓
CVE-2022-2161	Use after free in WebApp Provider	✓
CVE-2022-2162	Insufficient policy enforcement in File System API	✓
CVE-2022-2163	Use after free in Cast UI and Toolbar.	✓
CVE-2022-2164	Inappropriate implementation in Extensions API	✓
CVE-2022-2165	Insufficient data validation in URL formatting.	✓

# Technical Details

## #1

This update addressed nine vulnerabilities, the critical vulnerability CVE-2022-2156 could allow a remote attacker to create a specially crafted webpage and trick the victim into visiting it, followed by executing arbitrary code on the target system.

## #2

The vulnerabilities CVE-2022-2157 and CVE-2022-2158, could allow remote attackers to trigger type confusion or use-after-free flaws to execute arbitrary code on the vulnerable system. This advisory also addresses six more vulnerabilities that have been fixed by Chrome.

## Vulnerability Details

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2022-2156	Google Chromium: 103.0.5006.0 - 103.0.5030.1	cpe:2.3:a:google:chromium:*:*:*:*:*:*	CWE-416
CVE-2022-2157			CWE-416
CVE-2022-2158			CWE-843
CVE-2022-2160			CWE-264
CVE-2022-2158			CWE-843
CVE-2022-2160			CWE-264
CVE-2022-2161			CWE-416
CVE-2022-2162			CWE-264
CVE-2022-2163			CWE-416
CVE-2022-2164			CWE-358
CVE-2022-2165			CWE-20

## Patch Details

Update Google Chrome to version 103.0.5060.53

Patch Link

<https://www.google.com/intl/en/chrome/?standalone=1>

## References

[https://chromereleases.googleblog.com/2022/06/stable-channel-update-for-desktop\\_21.html](https://chromereleases.googleblog.com/2022/06/stable-channel-update-for-desktop_21.html)

# What Next?

Book a free demo with **HivePro Uni5** to check your exposure to this advisory. HivePro Uni5 is a Threat Exposure Management Solution that proactively reduces an organization's attack surface before it gets exploited.



At Hive Pro we take a long hard look at your vulnerabilities so you can bolster your defenses and fine-tune your offensive cybersecurity tactics.

REPORT GENERATED ON

**June 23, 2022 • 12:45 AM**

© 2022 All Rights are Reserved by HivePro



More at [www.hivepro.com](http://www.hivepro.com)