

THREAT ADVISORY



**VULNERABILITY
REPORT**

Zero-day vulnerability in Chrome browser being exploited-in-the-wild

Date of Publication

July 06, 2022

Admiralty code

A2


TA Number

TA2022140

Summary

The heap buffer overflow vulnerability in chrome browser let attackers to run arbitrary code or cause denial-of-service condition.

CVEs

CVE	NAME	PATCH
CVE-2022-2294	Heap buffer overflow in WebRTC	

Potential MITRE ATT&CK TTPs

TA0007 Discovery	T1518 Software Discovery	TA0040 Impact	TA0002 Execution	T1203 Exploitation for Client Execution
T1499 Endpoint Denial of Service	T1499.004 Endpoint Denial of Service: Application or System Exploitation			

Technical Details

The heap overflow vulnerability exists due to an error in the WebRTC component. The component has the capabilities to perform real time audio and video communication. The successful exploitation of this issue may lead to either arbitrary code execution or denial-of-service condition.

Vulnerability Details

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2022-2294	Google Chrome	cpe:2.3:a:google:google_chrome:*.*.*.*.*.*.*	CWE-122

Patch Details

Update to Google Chrome version 103.0.5060.114 for Windows, MacOS, and Linux.

References

<https://chromereleases.googleblog.com/2022/07/extended-stable-channel-update-for.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

July 06, 2022 • 5:45 AM

© 2022 All Rights are Reserved by HivePro



More at www.hivepro.com