Hive Pro

Threat Level

Red

THREAT ADVISORY

VULNERABILITY REPORT

Chrome's zero-day flaw allows arbitrary code execution

Date of Publication	Admiralty Code	TA Number
August 18, 2022	A1	TA2022175

Summary

A vulnerability(CVE-2022-2856) in Google Chrome, has been exploited in the wild. Additionally, Chrome has addressed several other use-after-free vulnerabilities in multiple components, including FedCM, SwiftShader, ANGLE, and Blink.

CVE Table

CVE	NAME	PATCH
CVE-2022-2856	Insufficient validation of untrusted input in Intents	✓
CVE-2022-2852	Use after free in FedCM	✓
CVE-2022-2854	Use after free in SwiftShader	✓
CVE-2022-2855	Use after free in ANGLE	✓
CVE-2022-2857	Use after free in Blink	✓
CVE-2022-2858	Use after free in Sign-In Flow	✓
CVE-2022-2853	Heap buffer overflow in Downloads	✓
CVE-2022-2859	Use after free in Chrome OS Shell	✓
CVE-2022-2860	Insufficient policy enforcement in Cookies	✓
CVE-2022-2861	Inappropriate implementation in Extensions API	✓

Potential MITRE ATT&CK TTPs

TA0005 Defense Evasion	**T1055** Process Injection	**TA0004** Privilege Escalation	**TA0001** Initial Access
T1190 Exploit Public-Facing Application	**TA0002** Execution	**T1203** Exploitation for Client Execution	**TA0042** Resource Development
T1608 Stage Capabilities	**T1608.004** Drive-by Target	**T1106** Native API	

Technical Details

#1 The zero-day (CVE-2022-2856) exists due to improper input validation in Google Chrome's Intents component. A remote attacker can deceive the victim into opening a specially constructed web page, allowing the attacker to execute arbitrary code on the target system.

#2 A use after free vulnerability in FedCM tagged as CVE-2022-2852 occurs from inappropriate use of dynamic memory during program execution. If the software does not delete the pointer to a memory address after freeing it, an attacker can use the error to alter the program.

#3 SwiftShader, an open-source library that provides 3D rendering software, has also been found to have a use-after-free flaw CVE-2022-2854. To trigger the issue and execute arbitrary code on the target system, the attacker would have to convince the victim to visit a specially designed website.

#4 CVE-2022-2853 is a heap-based buffer overflow issue caused by a boundary error when processing untrusted HTML input in Downloads. A remote actor that successfully exploits this vulnerability to execute arbitrary code.

Vulnerability Details

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2022-2856	Google Chromium: 104.0.5112.0 - 104.0.5112.100	cpe:2.3:a:google:chromium:104.0.5112.-:*:*:*:*:*:*:*	CWE-20
CVE-2022-2852	Google Chromium: 104.0.5112.0 - 104.0.5112.100	cpe:2.3:a:google:chromium:104.0.5112.-:*:*:*:*:*:*:*	CWE-416
CVE-2022-2854	Google Chromium: 104.0.5112.0 - 104.0.5112.100	cpe:2.3:a:google:chromium:104.0.5112.-:*:*:*:*:*:*:*	CWE-416

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2022-2855	Google Chromium: 104.0.5112.0 - 104.0.5112.100	cpe:2.3:a:google:chromium:104.0.5112.-:*:*:*:*:*:*:*	CWE-416
CVE-2022-2857	Google Chromium: 104.0.5112.0 - 104.0.5112.100	cpe:2.3:a:google:chromium:104.0.5112.-:*:*:*:*:*:*:*	CWE-416
CVE-2022-2858	Google Chromium: 104.0.5112.0 - 104.0.5112.100	cpe:2.3:a:google:chromium:104.0.5112.-:*:*:*:*:*:*:*	CWE-416
CVE-2022-2853	Google Chromium: 104.0.5112.0 - 104.0.5112.100	cpe:2.3:a:google:chromium:104.0.5112.-:*:*:*:*:*:*:*	CWE-122
CVE-2022-2859	Google Chromium: 104.0.5112.0 - 104.0.5112.100	cpe:2.3:a:google:chromium:104.0.5112.-:*:*:*:*:*:*:*	CWE-416
CVE-2022-2860	Google Chromium: 104.0.5112.0 - 104.0.5112.100	cpe:2.3:a:google:chromium:104.0.5112.-:*:*:*:*:*:*:*	CWE-264
CVE-2022-2861	Google Chromium: 104.0.5112.0 - 104.0.5112.100	cpe:2.3:a:google:chromium:104.0.5112.-:*:*:*:*:*:*:*	CWE-358

Patch Details

Update to Google Chrome version 104.0.5112.101 for Mac and Linux and 104.0.5112.102/101 for Windows

References

https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_16.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

August 18, 2022 • 3:55 AM

© 2022 All Rights are Reserved by HivePro

More at www.hivepro.com