Hive Pro

Threat Level

Green

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Chrome 110 Tackles a Collection of Security Weaknesses

Date of Publication	Admiralty code	TA Number
February 9, 2023	A1	TA2023071

Summary

First Seen: February 7, 2023
Affected Product: Google Chrome
Impact: Arbitrary code execution allows an attacker to gain access to sensitive information.

CVEs

CVE	NAME	PATCH
CVE-2023-0696	Type Confusion in V8	✓
CVE-2023-0697	Inappropriate implementation in Full screen mode	✓
CVE-2023-0698	Out of bounds read in WebRTC	✓
CVE-2023-0699	Use after free in GPU	✓
CVE-2023-0700	Inappropriate implementation in Download	✓
CVE-2023-0701	Heap buffer overflow in WebUI	✓
CVE-2023-0702	Type Confusion in Data Transfer	✓
CVE-2023-0703	Type Confusion in DevTools	✓
CVE-2023-0704	Insufficient policy enforcement in DevTools	✓
CVE-2023-0705	Integer overflow in Core	✓

Vulnerability Details

The latest stable channel update of Google Chrome, version 110, addresses various security weaknesses. A type confusion error in the V8 component, tracked under CVE-2023-0696, allows a malicious actor to create a specially crafted web page that, when visited by a victim, can trigger the error and execute arbitrary code on their system. The Full-screen mode in Google Chrome contains an incorrect implementation, tracked under CVE-2023-0697, that can be exploited by a remote attacker to compromise the victim's system through a similarly crafted web page. Additionally, an out-of-bounds read vulnerability in the WebRTC component, tracked under CVE-2023-0698, enables a remote attacker to access sensitive information by tricking the victim into visiting a specially crafted web page and triggering the error.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-0696	Google Chrome: 100.0.4896.60 - 109.0.5414.120	cpe:2.3:a:google:google_chrome:-:*:*:*:*:*:*:*	CWE-843
CVE-2023-0697			CWE-358
CVE-2023-0698			CWE-125
CVE-2023-0699			CWE-416
CVE-2023-0700			CWE-358
CVE-2023-0701			CWE-122
CVE-2023-0702			CWE-843
CVE-2023-0703			CWE-843
CVE-2023-0704			CWE-264
CVE-2023-0705			CWE-190

Recommendations

Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize the vulnerability, identify the impacted assets, and patch them through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Patch Details' on the following page.

Patch Details

Update Google Chrome to version 110.0.5481.77 for Mac/linux and 110.0.5481.77/.78 for Windows.

Patch Link
https://www.google.com/intl/en/chrome/?standalone=1

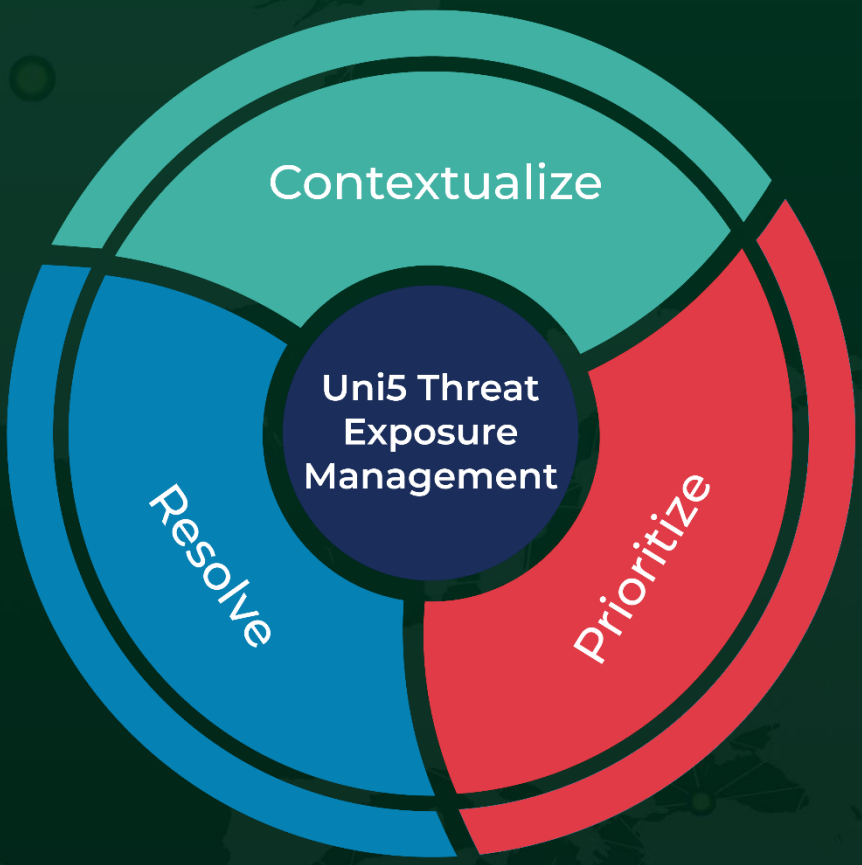
References

https://chromereleases.googleblog.com/2023/02/stable-channel-update-for-desktop.html

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

February 9, 2023 • 2:55 AM

More at www.hivepro.com