

HiveForce Labs

# THREAT ADVISORY

## VULNERABILITY REPORT

**Google releases Chrome 109 with a range of bug fixes**

Date of Publication

January 10, 2023

Admiralty code

A1

TA Number

TA2023017





# Summary

**First Seen:** January 10, 2022

**Affected Product:** Google Chrome

**Impact:** Arbitrary code execution

## CVEs

CVE	NAME	PATCH
CVE-2023-0128	Use after free in Overview Mode	
CVE-2023-0129	Heap buffer overflow in Network Service	
CVE-2023-0130	Inappropriate implementation in Fullscreen API	
CVE-2023-0131	Inappropriate implementation in iframe Sandbox	
CVE-2023-0132	Inappropriate implementation in Permission prompts	
CVE-2023-0133	Inappropriate implementation in Permission prompts	
CVE-2023-0134	Use after free in Cart	

CVE	NAME	PATCH
CVE-2023-0135	Use after free in Cart	✓
CVE-2023-0136	Inappropriate implementation in Fullscreen API	✓
CVE-2023-0137	Heap buffer overfin Platform Apps	✓
CVE-2023-0138	Heap buffer overfin libphonenumber	✓
CVE-2023-0139	Insufficient validation of untrusted input in Downloads	✓
CVE-2023-0140	Inappropriate implementation in File System API	✓
CVE-2023-0141	Insufficient policy enforcement in CORS	✓

# Vulnerability Details

Google Chrome 109 is being promoted to the stable channel for Windows, Mac, and Linux. It contains a number of bug fixes and improvements, including use after free in Overview Mode, a heap buffer overflow in Network Service, inappropriate implementation in Fullscreen API, use after free in Cart, heap buffer overflow in libphonenumber, insufficient validation of untrusted input in Downloads, and insufficient policy enforcement in CORS.



## Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-0128	Google Chrome: 100.0.4896.60 - 108.0.5359.125	cpe:2.3:a:google:google_chrome:- :*:*:*:*:*:*	CWE-416
CVE-2023-0129			CWE- 122
CVE-2023-0130			CWE-358
CVE-2023-0131			CWE-358
CVE-2023-0132			CWE-358
CVE-2023-0133			CWE-358
CVE-2023-0134			CWE-416
CVE-2023-0135			CWE-416
CVE-2023-0136			CWE-358
CVE-2023-0137			CWE- 122
CVE-2023-0138			CWE- 122
CVE-2023-0139			CWE-20
CVE-2023-0140			CWE-358
CVE-2023-0141			CWE-264

# 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 109.0.5414.74 (linux), 109.0.5414.74/.75 (Windows) and 109.0.5414.87 (Mac)

Patch Link

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

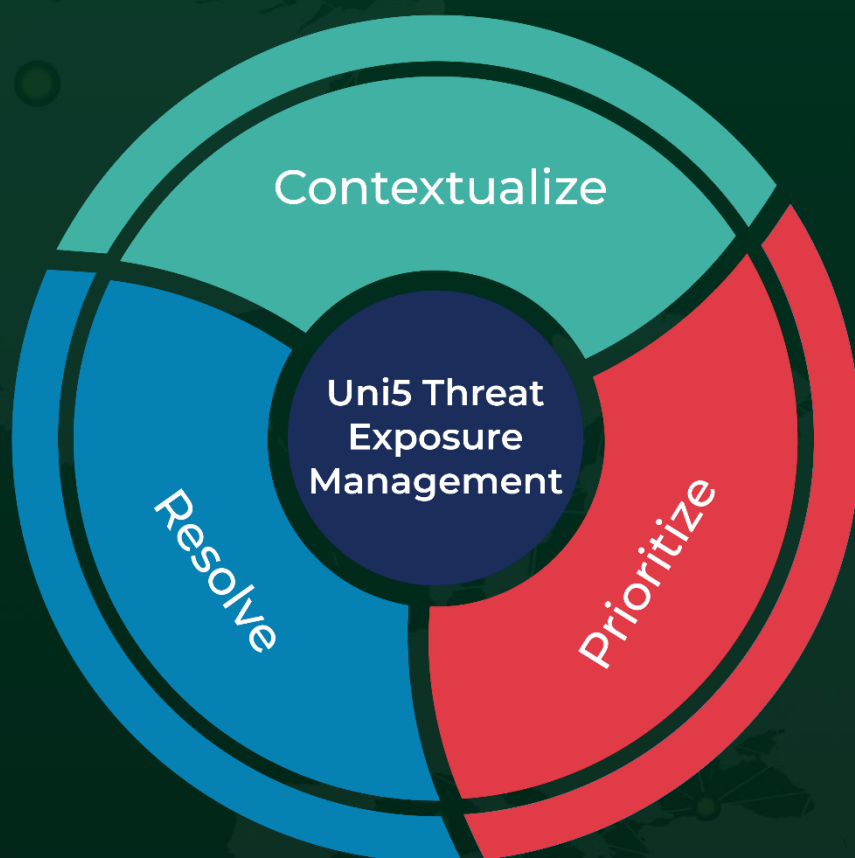
## References

<https://chromereleases.googleblog.com/2023/01/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

**January 10, 2023 • 11:45 PM**

© 2022 All Rights are Reserved by HivePro



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