Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Google's Battle Against Zero-Day Vulnerability Continues

Date of Publication	Admiralty Code	TA Number
December 21, 2023	A1	TA2023516

Summary

First Seen: December 20, 2023
Affected Product: Google Chrome
Affected Platforms: Windows, Mac, and Linux
Impact: Google has recently implemented a security enhancement to address a high-severity zero-day vulnerability, identified as CVE-2023-7024, that can lead to program crashes or enable arbitrary code execution.

⚙ CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-7024	Google Chrome Heap buffer overflow in WebRTC Vulnerability	Google Chrome	✓	✓	✓

Vulnerability Details

#1

Google has implemented a security update to address a zero-day vulnerability of significant severity capable of causing program crashes or enabling arbitrary code execution. This flaw has been actively exploited in the wild. Identified as CVE-2023-7024, the vulnerability manifests as a heap buffer overflow weakness within the open-source WebRTC framework, which is utilized by various web browsers, including Mozilla Firefox, Safari, and Microsoft Edge. WebRTC facilitates Real-Time Communications (RTC) through JavaScript APIs. Previously, CVE-2023-4762 gained attention as Google released its patch several weeks after the vulnerability was exploited by a threat actor to distribute sophisticated spyware named **Predator** across Android devices located in Egypt.

#2

Throughout the current year, Google has addressed and patched multiple actively exploited zero-day vulnerabilities in Chrome—identified as **CVE-2023-2033**, **CVE-2023-2136**, **CVE-2023-3079**, **CVE-2023-4863**, **CVE-2023-5217**, and **CVE-2023-6345**. These vulnerabilities were targeted in attacks, emphasizing the need to enhance the browser's security. Google has introduced updates for the Chrome Extended Stable channel, specifically version 120.0.6099.129 for macOS and version 120.0.6099.130 for Windows.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-7024	Google Chrome: 100.0.4896.60 - 120.0.6099.110	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	CWE-122

Recommendations

Apply Official Fixes Immediately: Ensure your Chrome browser is updated to the latest version (120.0.6099.129/130 for Windows and 120.0.6099.129 for Mac and Linux). Open Chrome, go to "Settings," scroll down to "About Chrome," and allow the browser to check for updates.

Keep Operating System Updated: Regularly update your operating system (Windows, macOS, or Linux) to apply the latest security patches and enhancements.

Use Security Software: Employ reputable antivirus and anti-malware software to add an extra layer of protection against potential threats.

Vulnerability Management: This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0040 Impact
T1059 Command and Scripting Interpreter	T1203 Exploitation for Client Execution	T1588 Obtain Capabilities	T1059 Command and Scripting Interpreter
T1588.005 Exploits	T1588.006 Vulnerabilities		

Patch Details

Update Chrome browser to the latest version 120.0.6099.129/130 for Windows and 120.0.6099.129 for Mac and Linux

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

References

https://chromereleases.googleblog.com/2023/12/stable-channel-update-for-desktop_20.html

https://chromereleases.googleblog.com/

https://www.hivepro.com/threat-advisory/apple-addresses-zero-day-flaws-exploited-in-the-wild/

https://www.hivepro.com/threat-advisory/google-chrome-emergency-update-fixes-zero-day-exploit-in-the-wild/

https://www.hivepro.com/threat-digest/cisa-known-exploited-vulnerability-catalog-april-2023/

https://www.hivepro.com/threat-advisory/google-addresses-high-stakes-chrome-zero-day-vulnerability/

https://www.hivepro.com/threat-advisory/google-addresses-fourth-zero-day-flaw-exploited-by-attackers-wildly/

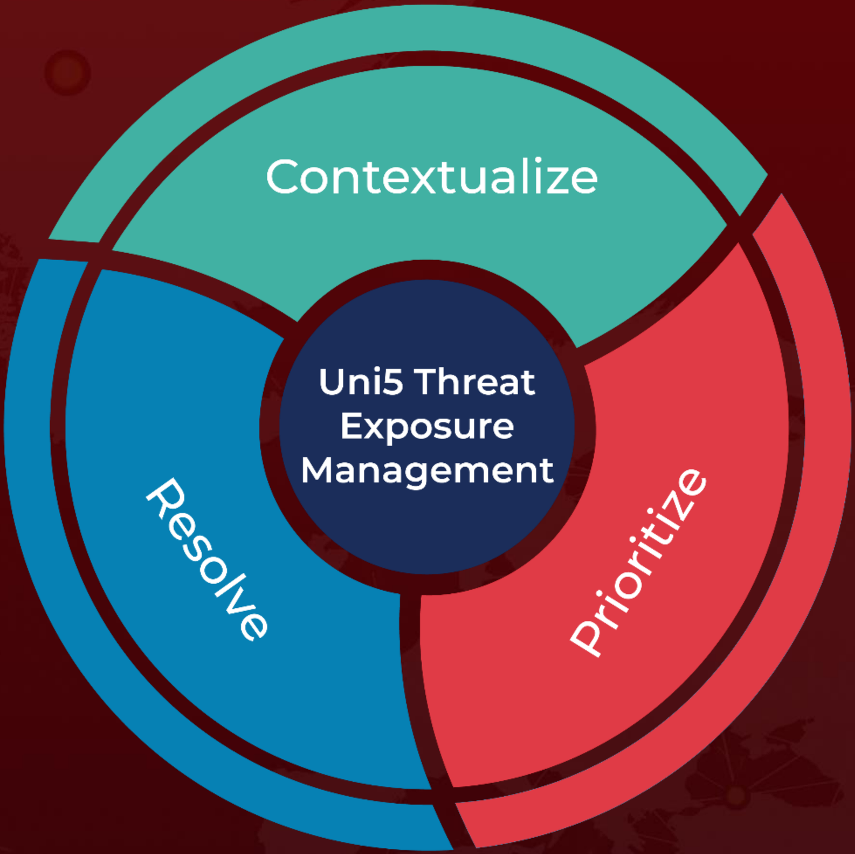
https://www.hivepro.com/threat-advisory/google-and-firefox-fixes-zero-day-flaw-exploited-in-the-wild/

https://www.hivepro.com/threat-advisory/google-addresses-sixth-zero-day-flaw-exploited-by-attackers-wildly/

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

December 21, 2023 • 9:00 PM

More at www.hivepro.com