Hive Pro

HiveForce Labs
THREAT ADVISORY

🐛 VULNERABILITY REPORT

Google Addresses High-Stakes Chrome Zero-Day Vulnerability

Date of Publication	Admiralty Code	TA Number
June 7, 2023	A1	TA2023254

Summary

First Seen: June 5, 2023
Affected Product: Google Chrome web browser
Affected Platforms: Windows, Mac, and Linux
Impact: The vulnerability could allow attackers to execute arbitrary code, which could potentially lead to data theft, system compromise, and other malicious activities.

☼ CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-3079	Google Chrome Type Confusion Vulnerability	Google Chromium V8 Engine	✅	✅	✅

Vulnerability Details

#1 The CVE-2023-3079 vulnerability is a high-severity zero-day, marking it as the third zero-day vulnerability affecting Chrome since the beginning of 2023. This vulnerability revolves around a type confusion weakness within the Chrome V8 JavaScript engine. If successfully exploited, it grants attackers the ability to execute arbitrary code on compromised devices. Type confusion flaws occur when the engine incorrectly interprets the type of an object during runtime, potentially resulting in manipulative memory actions and the execution of unauthorized code.

#2 Google has confirmed the existence of an exploit for this vulnerability in the wild. Zero-day vulnerabilities are frequently targeted by sophisticated threat actors, often backed by state-sponsored entities, with a primary focus on prominent individuals within governmental, media, or other critical organizations. Consequently, it is strongly advised that all Chrome users promptly install the provided security update.

✺ Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-3079	Google Chrome: 100.0.4896.60 - 114.0.5735.91	cpe:2.3:a:google:google_chrome:-:*:*:*:*:*:*:*	CWE-843

Recommendations

Update to the latest version: Users are highly recommended to upgrade their Chrome browser to the latest versions available - version 114.0.5735.110 for Windows and 114.0.5735.106 for macOS and Linux. These updates contain crucial **fixes** that effectively mitigate potential threats related to the vulnerability.

Keep your Chromium-based browser up to date: Users of Chromium-based browsers, including Microsoft Edge, Brave, Opera, and Vivaldi, should promptly apply any available fixes as soon as they are released. Ensuring that your browser is regularly updated is crucial for maintaining a secure browsing experience.

Evaluate the option of disabling JavaScript: Considering that the vulnerability is rooted in the Chrome V8 JavaScript engine, temporarily disabling JavaScript can help decrease the likelihood of exploitation. However, it is crucial to be aware that disabling JavaScript might impact the functionality of specific websites and web applications. Before choosing this solution, users should assess the potential impact on their browsing experience and determine if it is a practical measure for them.

⚛ Potential MITRE ATT&CK TTPs

TA0005 Defense Evasion	TA0004 Privilege Escalation	TA0002 Execution	TA0040 Impact
TA0003 Persistence	T1203 Exploitation for Client Execution	T1068 Exploitation for Privilege Escalation	T1190 Exploit Public-Facing Application
T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1588.005 Exploits	

✂ Patch Links

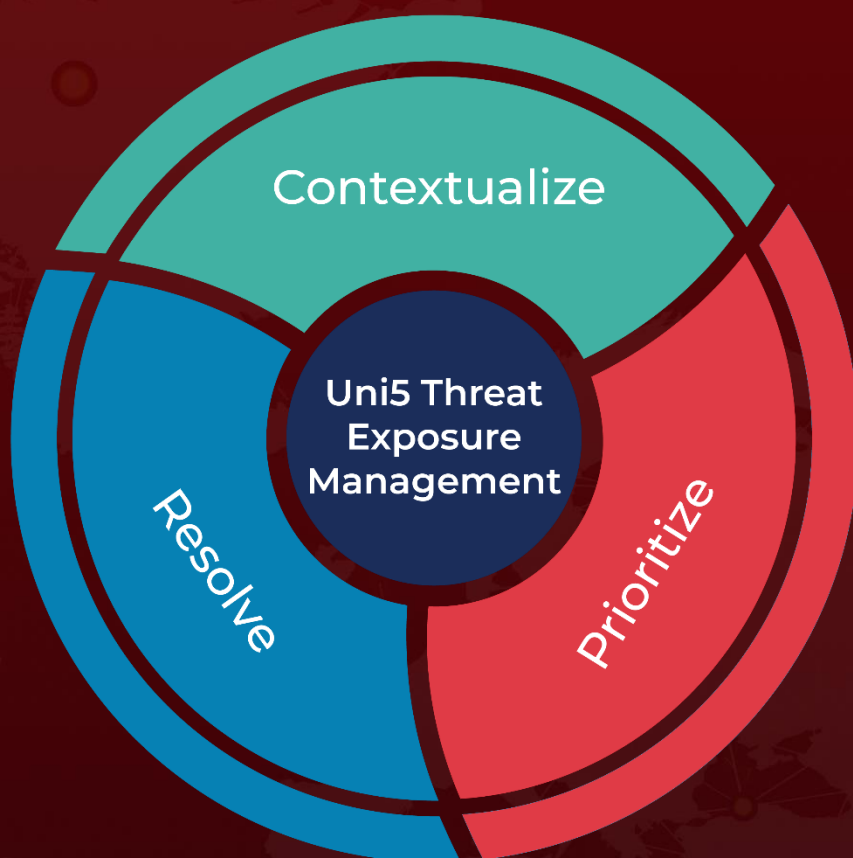https://www.google.com/intl/en/chrome/?standalone=1

✂ References

https://chromereleases.googleblog.com/2023/06/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.

More at www.hivepro.com