

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Google Chrome Emergency Update Fixes Zero-Day Exploit in the Wild

Date of Publication

April 17, 2023

Admiralty Code

A1

TA Number

TA2023188

Summary




First Seen: April 11, 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.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-2033	Google Chrome Type Confusion Vulnerability	Google Chrome			

Vulnerability Details

The CVE-2023-2033 vulnerability is a high-severity zero-day vulnerability that was exploited in attacks, making it the first zero-day chrome vulnerability to be exploited since the start of the year 2023. The vulnerability is related to a type confusion weakness in the Chrome V8 JavaScript engine, which could allow attackers to execute arbitrary code on compromised devices. Google has acknowledged that there is an exploit for this vulnerability in the wild. Google has released an emergency Chrome security update to address this vulnerability and has advised Chrome users to upgrade to version 112.0.5615.121 as soon as possible.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-2033	Google Chrome: All versions (before 112.0.5615.121)	cpe:2.3:a:google:google_chrome:~:*:*:*:*:*	CWE-843

Recommendations



The best way to protect against this vulnerability is to update Google Chrome to the latest version (112.0.5615.121) as soon as possible. Users can do this by opening the Chrome menu, selecting Help, and then selecting About Google Chrome. If an update is available, it will be installed automatically.



Disable JavaScript, since this vulnerability is caused by a weakness in the Chrome V8 JavaScript engine, disabling JavaScript can help mitigate the risk of exploitation. However, this may also affect the functionality of certain websites and web applications, so it may not be a practical solution for all users.



Enable site isolation, is a security feature in Google Chrome that can help prevent attackers from exploiting vulnerabilities like CVE-2023-2033. Users can enable site isolation by going to `chrome://flags/#enable-site-per-process` in the Chrome address bar and enabling the feature.



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 Details

Upgrade the chromium package to version 112.0.5615.121.
<https://www.google.com/intl/en/chrome/?standalone=1>



References

https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop_14.html

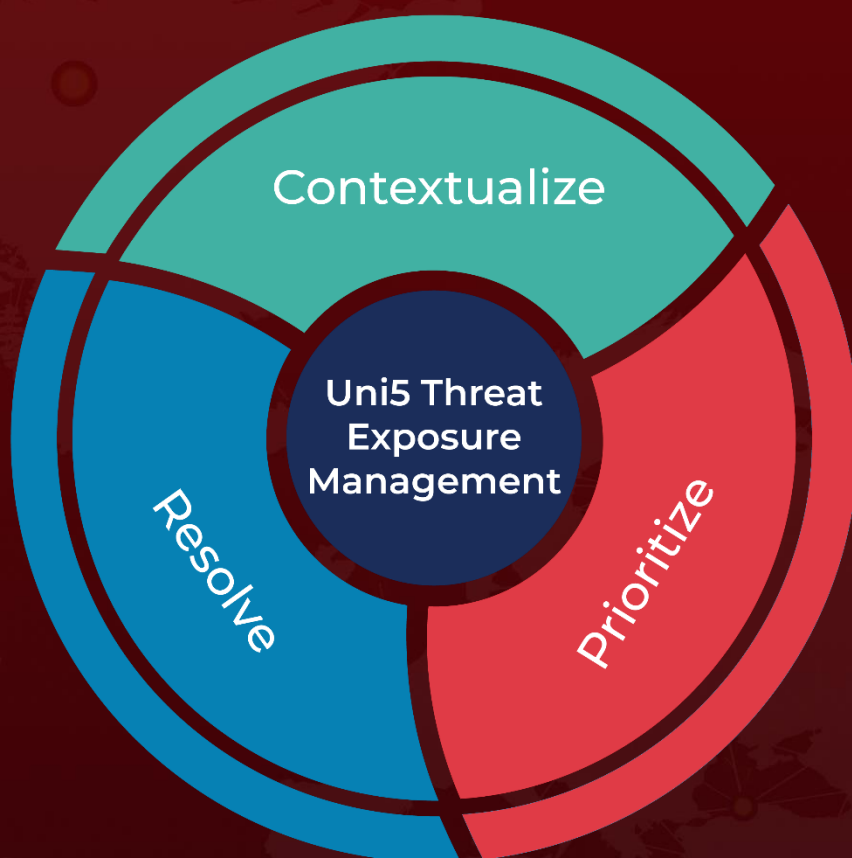
<https://www.bleepingcomputer.com/news/security/google-chrome-emergency-update-fixes-first-zero-day-of-2023/>

<https://www.cisa.gov/news-events/alerts/2023/04/17/cisa-adds-two-known-exploited-vulnerabilities-catalog>

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

April 17, 2023 • 12:30 AM

© 2023 All Rights are Reserved by HivePro



More at www.hivepro.com