

HiveForce Labs

THREAT ADVISORY



VULNERABILITY REPORT

Google Addresses Fourth Zero-Day Flaw Exploited by Attackers Wildly

Date of Publication

September 12, 2023

Admiralty Code

A1

TA Number

TA2023365




Summary

First Seen: September 6, 2023

Affected Platforms: Google Chrome

Impact: The zero-day vulnerability (CVE-2023-4863) enabling arbitrary code execution and system crashes. Actively exploited "in the wild," it poses severe risks, including data exposure and potential targeted attacks. Immediate patching and security vigilance are essential to mitigate these threats.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-4863	Google Chrome Heap Buffer Overflow Vulnerability	Google Chrome			

Vulnerability Details

#1

A heap buffer overflow zero-day vulnerability identified as 'CVE-2023-4863' in the WebP image format that affects Google Chrome. A heap buffer overflow occurs when a program writes more data to a buffer located in the heap than what is actually allocated for that buffer. This can corrupt the data of nearby buffers and cause unexpected behavior or crashes.

#2

An attacker can exploit this vulnerability to execute arbitrary code on the target system by crafting a malicious WebP image and convincing a user to view it on Chrome. This could compromise the security and privacy of the user and their data.

#3

The vulnerability is also being exploited in the wild by unknown threat actors, which increases the risk of exposure for Chrome users. Google has confirmed that this vulnerability is being exploited in the wild by unknown threat actors and has released a patch on September 11, 2023. This is the fourth zero-day vulnerability that Google patched in Chrome in 2023, indicating a high level of interest and sophistication from the attackers

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-4863	Google Chrome version 116.0.5845.186 and before	cpe:2.3:a:google:chrome:*:*:*:*:*:* e.*:*:*:*:*:*:*	CWE-122

Recommendations



Apply Immediate Security Patch: To protect against this critical vulnerability, it is imperative to apply the security patch provided by the relevant software vendor promptly. Ensure that all systems and applications using the WebP image format are updated to the latest secure version.



Enhance Security Hygiene: In addition to patching, bolster your overall security posture. Regularly update and maintain all software and applications on your systems to minimize potential vulnerabilities. Employ robust and up-to-date antivirus and intrusion detection systems to detect and prevent malware.



Exercise Caution Online: Be cautious when browsing the web and opening files from untrusted sources. Avoid clicking on suspicious links or downloading files from unknown websites or email attachments. User awareness and vigilance are crucial in preventing potential exploits of this vulnerability.

Potential MITRE ATT&CK TTPs

<u>TA0042</u> Resource Development	<u>TA0040</u> Impact	<u>TA0001</u> Initial Access	<u>TA0002</u> Execution
<u>T1588</u> Obtain Capabilities	<u>T1588</u> Obtain Capabilities	<u>T1588.005</u> Exploits	<u>T1059</u> Command and Scripting Interpreter
<u>T1189</u> Drive-by Compromise			

Patch Details

Upgrade to Chrome version 116.0.5845.187/.188 for Windows and 116.0.5845.187 for macOS and Linux

Link:

https://chromereleases.googleblog.com/2023/09/stable-channel-update-for-desktop_11.html

References

<https://securityaffairs.com/150657/hacking/google-fixed-the-fourth-chrome-zero-day-of-2023.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

September 12, 2023 • 5:00 AM

© 2023 All Rights are Reserved by HivePro®



More at www.hivepro.com