

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Yet Another Google Chrome Zero-Day Exploited in the Wild

Date of Publication

May 14, 2024

Last Update Date

May 16, 2024

Admiralty Code

A1

TA Number

TA2024186

Summary

Discovered: 9 May 2024

Affected Products: Google Chrome

Impact: Google has released emergency security patches for the Chrome browser to address zero-day vulnerabilities, CVE-2024-4761 and CVE-2024-4947, both of which have been exploited in attacks. These vulnerabilities affect Chrome's V8 JavaScript engine, which is responsible for executing JavaScript code within the application. CVE-2024-4761 is classified as an out-of-bounds write vulnerability, while CVE-2024-4947 is classified as a Type Confusion vulnerability.

⚙️ CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-4761	Google Chrome Out of bounds write in V8 Vulnerability	Google Chrome	✓	✓	✓
CVE-2024-4947	Google Chrome Type Confusion in V8 Vulnerability	Google Chrome	✓	✓	✓

Vulnerability Details

#1

CVE-2024-4761, a newly discovered zero-day vulnerability in Chrome's V8 JavaScript engine, has been swiftly addressed. This vulnerability, classified as an out-of-bounds write issue, poses a serious threat by enabling remote attackers to compromise systems. Exploiting untrusted HTML content in V8, attackers can manipulate webpages to trigger arbitrary code execution on victims' machines, exploiting a boundary error. Notably, an active exploit for this vulnerability is already circulating in the wild.

#2

Within just days of addressing CVE-2024-4761, Google faced another critical issue and provided updates to thwart the widespread exploitation of yet another zero-day vulnerability, CVE-2024-4947. This new flaw originated from a type confusion bug within V8. Exploiting this vulnerability allowed remote attackers to execute arbitrary code within a sandbox environment by utilizing carefully crafted HTML pages.

#3

While vulnerabilities of this nature typically lead to browser crashes, threat actors can exploit them for more severe consequences, including arbitrary code execution on targeted devices. To safeguard against such risks, ensure your browser is updated to version 125.0.6422.60/.61 for Mac/Windows and 125.0.6422.60 for Linux.

#4

Google has addressed three zero-day flaws, namely [CVE-2024-4671](#), CVE-2024-4761, and CVE-2024-4947, all within a span of one week, with multiple zero-days lingering within a week requiring users to be extra vigilant and cautious against phishing sites.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-4761	Google Chrome prior to 124.0.6367.207	cpe:2.3:a:google:chrome:*:*:*:*:*:*	CWE-787
CVE-2024-4947	Google Chrome prior to 125.0.6422.60	cpe:2.3:a:google:chrome:*:*:*:*:*:*	CWE-843

Recommendations



Update Chrome Immediately: Ensure that all systems running Google Chrome are updated to version 125.0.6422.60/.61 for Windows and Mac, or 125.0.6422.60 for Linux. Promptly apply any security updates released by Google to stay protected against known vulnerabilities.



Enable Automatic Updates: Configure Chrome to automatically install updates to ensure that security patches are applied as soon as they become available, reducing the window of exposure to potential threats.



Vulnerability Management: Implement a robust vulnerability management process to ensure that software and systems are regularly assessed for vulnerabilities and updated with the required security patches. Prioritize critical vulnerabilities identified by security advisories and vendors to mitigate the risk of exploitation by threat actors.



Network Segmentation: Implement network segmentation to isolate critical infrastructure components from other systems. This can limit lateral movement for attackers and contain potential breaches.

Potential MITRE ATT&CK TTPs

<u>TA0042</u> Resource Development	<u>TA0001</u> Initial Access	<u>TA0002</u> Execution	<u>T1588</u> Obtain Capabilities
<u>T1588.006</u> Vulnerabilities	<u>T1059</u> Command and Scripting Interpreter	<u>T1059.007</u> JavaScript	<u>T1566</u> Phishing
<u>T1204</u> User Execution	<u>T1189</u> Drive-by Compromise	<u>T1203</u> Exploitation for Client Execution	

Patch Details

Update Chrome browser to the latest version 125.0.6422.60/.61 for Mac and Windows and 125.0.6422.60 for Linux.

Links:

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

References

https://chromereleases.googleblog.com/2024/05/stable-channel-update-for-desktop_13.html

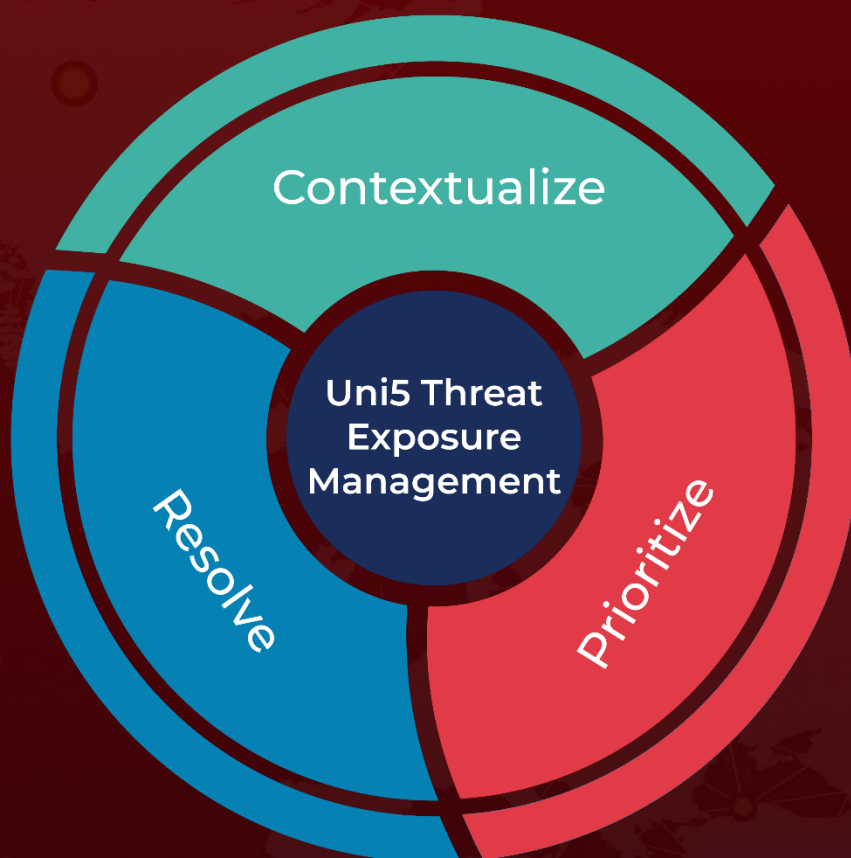
<https://www.hivepro.com/threat-advisory/google-chrome-fixes-zero-day-cve-2024-4671-exploited-in-the-wild/>

https://chromereleases.googleblog.com/2024/05/stable-channel-update-for-desktop_15.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

May 14, 2024 • 7:00 AM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com