

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Google Alerts Users to Actively Exploited Chrome Zero-Day Flaws

Date of Publication
August 22, 2024

Last Update Date
August 27, 2024

Admiralty Code
A1

TA Number
TA2024323







Summary

First Seen: August 2024

Affected Product: Google Chrome

Impact: Google has released a patch for two critical zero-day vulnerabilities in its Chrome browser, identified as CVE-2024-7971 and CVE-2024-7965. These high-severity flaws stem from improper implementations in Chrome's V8 JavaScript engine. CVE-2024-7971 could allow remote attackers to execute arbitrary code through a type confusion error, while CVE-2024-7965 could enable attackers to exploit heap corruption using a specially crafted HTML page. Both vulnerabilities have been actively exploited in the wild, highlighting the urgent need for users to update their browsers to the latest version immediately.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-7971	Google Chromium V8 Type Confusion Vulnerability	Google Chrome, Microsoft Edge			
CVE-2024-7965	Google Chrome's V8 JavaScript Engine Inappropriate Implementation Vulnerability	Google Chrome, Microsoft Edge			

Vulnerability Details

#1

Google has patched two critical zero-day vulnerabilities in its Chrome browser, identified as CVE-2024-7971 and CVE-2024-7965. These high-severity flaws affect Chrome versions earlier than 128.0.6613.84 and have been actively exploited in the wild, underscoring the urgency for users to update their browsers immediately to protect against potential attacks.

#2

The implications of CVE-2024-7971 are significant, as successful exploitation could allow attackers to execute malicious code, leading to unauthorized access to sensitive data or control over the affected system. This poses a serious threat to both individual users and organizations relying on Chrome for their online activities.

#3

CVE-2024-7965 is a vulnerability in Chrome's V8 JavaScript engine that allows a remote attacker to compromise the affected system due to an incorrect implementation in V8. By creating a specially crafted web page and tricking the victim into visiting it, an attacker can exploit this flaw to gain control of the system. This inappropriate implementation in V8 allowed remote attackers to potentially exploit heap corruption via a crafted HTML page.

#4

Google has addressed these issues in Chrome versions 128.0.6613.84/.85 for Windows and macOS, and 128.0.6613.84 for Linux. V8 powers Chrome and other Chromium-based browsers like Microsoft Edge. Both vulnerabilities have been actively exploited in the wild, making it crucial for users to apply these updates to safeguard their systems.

#5

Google has also addressed multiple other flaws in Chrome in 2024, including [CVE-2024-0519](#), [CVE-2024-2886](#), [CVE-2024-2887](#), [CVE-2024-3159](#), [CVE-2024-4671](#), [CVE-2024-4761](#), [CVE-2024-4947](#), and [CVE-2024-5274](#). This series of critical patches underscores the importance of regularly updating browsers to enhance security.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-7971	Google Chrome V8 prior to 128.0.6613.84 Microsoft Edge Version prior to 128.0.2739.42	cpe:2.3:a:google:chrome:*:*:*:*:*:* cpe:2.3:a:microsoft:edge:*:*:*:*:*:*	CWE-843
CVE-2024-7965	Google Chrome V8 prior to 128.0.6613.84 Microsoft Edge Version prior 128.0.2739.42	cpe:2.3:a:google:chrome:*:*:*:*:*:* cpe:2.3:a:microsoft:edge:*:*:*:*:*:*	CWE-358

Recommendations



Update Chrome Immediately: Ensure your Chrome browser is updated to version 128.0.6613.84 (Linux) or 128.0.6613.84/.85 (Windows and macOS) or later. This version contains the patch for the CVE-2024-7971 & CVE-2024-7965 vulnerabilities. You can update by navigating to Chrome Menu > Help > About Google Chrome, then letting the update process complete and clicking the 'Relaunch' button.



Enable Automatic Updates: Keep Chrome's automatic update feature enabled. This ensures that your browser always has the latest security patches and reduces the risk of falling victim to zero-day exploits.



Exercise Caution with Untrusted Websites: Be cautious when visiting unfamiliar or untrusted websites, as this vulnerability can be exploited through specially crafted web pages. Avoid clicking on suspicious links, especially those received through email or social media.



Security Software: Use reputable antivirus and anti-malware software. Regularly update and run scans to detect and remove potential threats.

Potential MITRE ATT&CK TTPs

<u>TA0002</u> Execution	<u>TA0040</u> Impact	<u>TA0042</u> Resource Development	<u>TA0001</u> Initial Access
<u>T1203</u> Exploitation for Client Execution	<u>T1204.001</u> Malicious Link	<u>T1059</u> Command and Scripting Interpreter	<u>T1588.005</u> Exploits
<u>T1204</u> User Execution	<u>T1189</u> Drive-by Compromise	<u>T1588</u> Obtain Capabilities	<u>T1588.006</u> Vulnerabilities

Patch Details

Update Google Chrome and Edge browser to latest version 128.0.6613.84 for Linux, 128.0.6613.84/.85 for Mac and Windows.

Link:

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

References

https://chromereleases.googleblog.com/2024/08/stable-channel-update-for-desktop_21.html

<https://www.hivepro.com/threat-advisory/google-fixes-first-actively-exploited-chrome-zero-day-of-2024/>

<https://www.hivepro.com/threat-advisory/google-patches-critical-zero-day-exploits-found-at-pwn2own/>

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

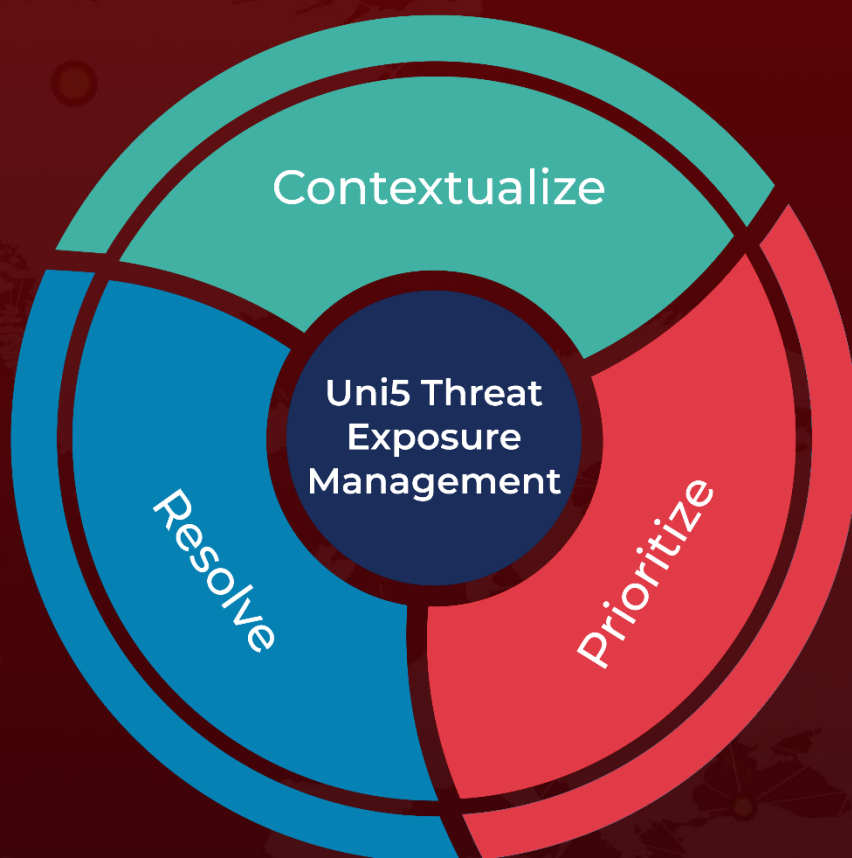
<https://www.hivepro.com/threat-advisory/yet-another-google-chrome-zero-day-exploited-in-the-wild/>

<https://www.hivepro.com/threat-advisory/google-fends-off-fourth-zero-day-in-may/>

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

August 22, 2024 • 4:30 AM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com