

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Critical Chromium Flaws Expose Systems to Code Execution Attacks

Date of Publication

October 4, 2024

Admiralty Code

A1

TA Number

TA2024380

Summary

First Seen: September 2024

Affected Products: Google Chrome, Microsoft Edge

Impact: Google has released a critical security update for Chromium, addressing multiple high-severity vulnerabilities. These flaws, if exploited, could enable attackers to execute arbitrary code on users' systems, putting sensitive data and system integrity at risk. Chromium users are advised to update their browsers immediately to ensure their devices are protected from potential threats.

⚙️ CVEs

CVE	NAME	AFFECTED PRODUCTS	ZERO-DAY	CISA	PATCH
CVE-2024-7025	Google Chrome Integer Overflow in Layout Vulnerability	Google Chrome, Microsoft Edge	✗	✗	✓
CVE-2024-9369	Google Chrome Insufficient Data Validation in Mojo Vulnerability		✗	✗	✓
CVE-2024-9370	Google Chrome Inappropriate Implementation in V8 Vulnerability		✗	✗	✓

Vulnerability Details

#1

Several high-severity vulnerabilities have been identified in Google Chromium, posing significant risks to system security. The flaws tracked as CVE-2024-7025, CVE-2024-9369, and CVE-2024-9370, could allow attackers to execute arbitrary code on affected systems potentially leading to full system compromise. Immediate updates are strongly recommended to mitigate the risks of exploitation. Notably, these flaws impact both Google Chrome and Microsoft Edge.

#2

CVE-2024-7025 represents a critical integer overflow vulnerability in the Layout component of Google Chrome. This flaw arises from the improper handling of integer values, which can exceed the maximum representable integer size. Attackers can exploit this vulnerability to manipulate memory, potentially leading to RCE. Such exploitation may allow unauthorized users to gain control over affected systems, posing significant security risks.

#3

CVE-2024-9369 is another high-severity vulnerability stems from insufficient data validation in the Mojo component of Chrome. Insufficient validation can lead to various security issues, including potential arbitrary code execution. Similar to CVE-2024-7025, successful exploitation could allow attackers to run arbitrary code with the privileges of the logged-in user. Depending on user rights, this could lead to severe consequences for system integrity and data security.

#4

The third identified vulnerability, CVE-2024-9370, resides in the V8 JavaScript engine. The inappropriate implementation in V8 can lead to various issues, including flawed handling of JavaScript objects or incorrect processing of specific operations. These weaknesses may result in unexpected behaviors when JavaScript code is executed, creating potential security concerns for users and systems alike.

#5

To mitigate the impact of these vulnerabilities, users are strongly urged to promptly apply the latest security updates for Google Chrome. It is essential for users to maintain minimal privileges and stay current with patches to effectively reduce the risk associated with these vulnerabilities.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-7025	Google Chrome Version prior to 129.0.6668.89/.90 for Windows and Mac Chrome prior to 129.0.6668.89 for Linux, Microsoft Edge Version prior to 129.0.2792.79	cpe:2.3:a:google:google_chrome:* :*:*:*:* cpe:2.3:a:microsoft:edge :*:*:*:*:*	CWE-190
CVE-2024-9369		cpe:2.3:a:google:google_chrome:* :*:*:*:* cpe:2.3:a:microsoft:edge :*:*:*:*:*	CWE-20
CVE-2024-9370		cpe:2.3:a:google:google_chrome:* :*:*:*:* cpe:2.3:a:microsoft:edge :*:*:*:*:*	CWE-358

Recommendations



Update Immediately: Ensure your Chrome browser is updated to version 129.0.6668.89 (Linux) or 129.0.6668.89/.90 (Windows and macOS) or later. This version contains the patch for the vulnerabilities. You can update by navigating to Chrome Menu > Help > About Google Chrome, then letting the update process complete and clicking the 'Relaunch' button. Update your Microsoft Edge to the latest version 129.0.2792.79.



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 exploits.



Least Privilege: Adhere to the idea of "least privilege" by giving users only the essential permissions they need for their tasks, restrict the access to the trusted parties only. This strategy reduces the effects of vulnerabilities related to privilege escalation.



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.

Potential MITRE ATT&CK TTPs

<u>TA0042</u> Resource Development	<u>TA0001</u> Initial Access	<u>TA0002</u> Execution	<u>TA0004</u> Privilege Escalation
<u>T1588</u> Obtain Capabilities	<u>T1588.006</u> Vulnerabilities	<u>T1190</u> Exploit Public-Facing Application	<u>T1059</u> Command and Scripting Interpreter
<u>T1068</u> Exploitation for Privilege Escalation			

Patch Details

Update Google Chrome to latest version 129.0.6668.89/.90 for Windows, Mac and 129.0.6668.89 for Linux.

Update your Microsoft Edge to latest version 129.0.2792.79.

Links:

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

<https://www.microsoft.com/en-us/edge/download?form=MA13FW>

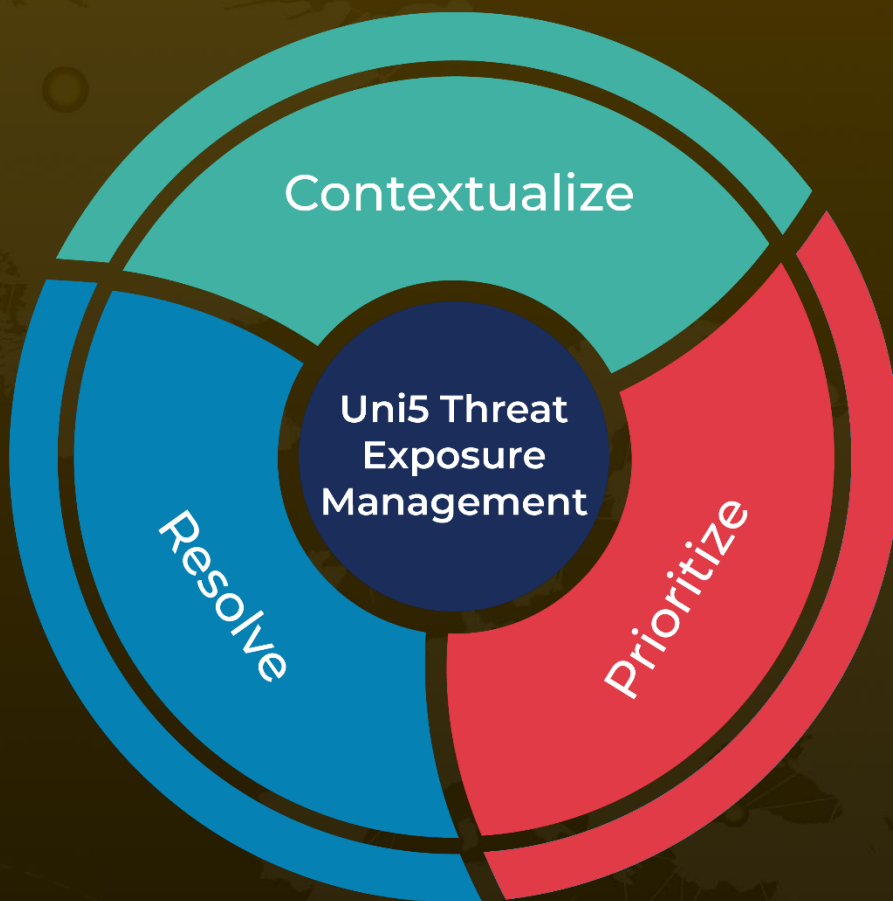
References

<https://chromereleases.googleblog.com/2024/10/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.



REPORT GENERATED ON

October 4, 2024 • 8:15 PM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com