Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Google Fends Off Fourth Zero-Day in May

Date of Publication	Admiralty Code	TA Number
May 27, 2024	A1	TA2024208

Summary

First Seen: May 23, 2024
Affected Product: Google Chrome
Impact: Google has addressed its eighth critical zero-day vulnerability of the year in the Chrome browser, designated as CVE-2024-5274. This defect pertains to a type confusion bug in the V8 JavaScript and WebAssembly engine that can lead to code execution, which underpins Chrome and other Chromium-based browsers, such as Microsoft Edge.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-5274	Google Chrome Type Confusion in V8 Vulnerability	Google Chrome	✓	✗	✓

Vulnerability Details

#1 For the eighth time this year, Google has addressed a critical zero-day vulnerability in its Chrome browser that has been actively exploited. This flaw, identified as CVE-2024-5274, involves a type confusion bug in the V8 JavaScript and WebAssembly engine. V8 powers Chrome and other Chromium-based browsers like Microsoft Edge. The type confusion attack vector is particularly perilous because it can lead to code execution when a user visits a maliciously crafted HTML page.

#2 A "type confusion" vulnerability arises when a program allocates memory for one type of data but mistakenly interprets it as another type. This can result in crashes, data corruption, and the execution of arbitrary code on the affected system. This development marks the fourth zero-day vulnerability that Google has patched this month, following CVE-2024-4671, CVE-2024-4761, and CVE-2024-4947.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-5274	Google Chrome version prior to 125.0.6422.112	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	CWE-843

Recommendations

Update Chrome Immediately: Ensure that all systems running Google Chrome are updated to version 125.0.6422.112/.113 for Windows and Mac, or 125.0.6422.112 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.

Implement Browser Isolation: Consider deploying browser isolation solutions that isolate web browsing activities from the endpoint to prevent zero-day exploits from reaching critical systems. Browser isolation technologies execute web code in a virtualized environment, reducing the attack surface and minimizing the impact of potential vulnerabilities.

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

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

Patch Details

Update Chrome browser to the latest version 125.0.6422.112/.113 for Mac and Windows and 125.0.6422.112 for Linux.

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

References

https://chromereleases.googleblog.com/2024/05/stable-channel-update-for-desktop_23.html

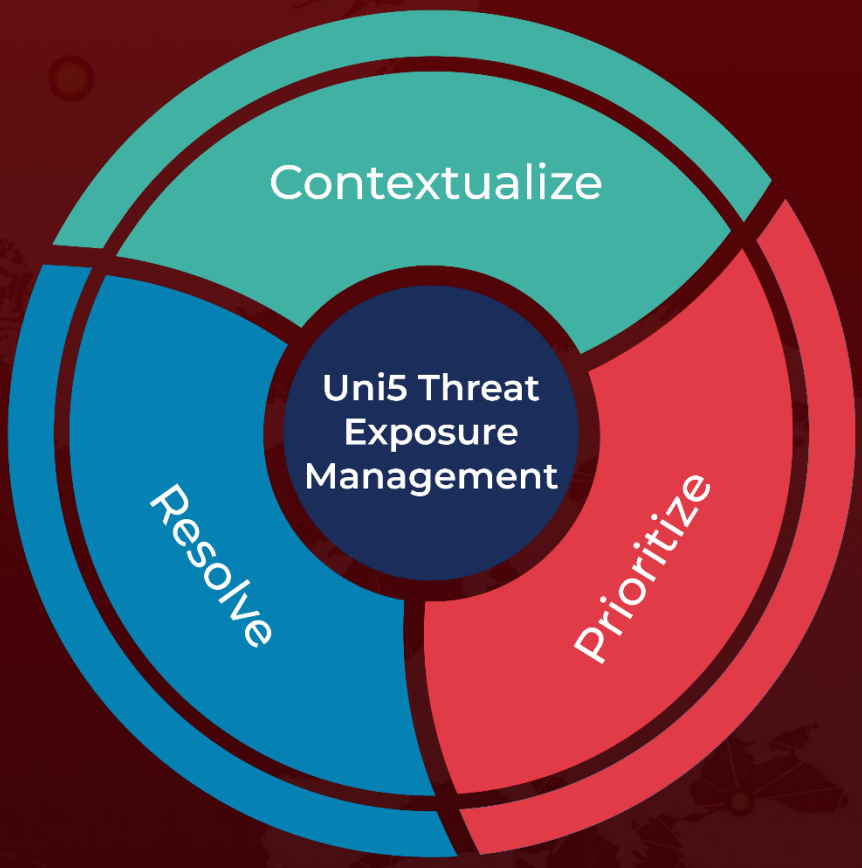
https://www.hivepro.com/threat-advisory/google-chrome-fixes-zero-day-cve-2024-4671-exploited-in-the-wild/

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

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 27, 2024 • 6:30 AM

More at www.hivepro.com