

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Google Fixes First Actively Exploited Chrome Zero-day of 2024

Date of Publication

January 17, 2024

Admiralty Code

A1

TA Number

TA2024019










Summary

First Seen: January 11, 2023

Affected Platform: Google Chrome

Impact: Google has addressed the first actively exploited Chrome zero-day vulnerability of 2024, identified as CVE-2024-0519. It's a high-severity 'out-of-bounds memory access' weakness in Chrome's V8. Attackers could exploit it to access data beyond the intended memory buffer, potentially leaking sensitive information or causing the browser to crash.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-0519	Google Chrome Out of bounds memory access Vulnerability	Google Chrome			
CVE-2024-0518	Google Chrome Type Confusion Vulnerability	Google Chrome			
CVE-2024-0517	Google Chrome Out of bounds write Vulnerability	Google Chrome			

Vulnerability Details

#1

Google has addressed a zero-day vulnerability, CVE-2024-0519, in its Chrome browser, marking the first such exploit encountered in the wild this year. The high-severity flaw is related to an out-of-bounds memory access weakness in the Chrome V8, allows a remote attacker to potentially exploit heap corruption via a crafted HTML page.

#2

Google released security updates for the Stable Desktop channel on Windows (version 120.0.6099.224/225), Mac (120.0.6099.234), and Linux (120.0.6099.224) within a week of discovering the issue. The company warns that updates may take time to reach all users but can be manually applied or set for automatic installation.

#3

Additionally, Google patched two other vulnerabilities, CVE-2024-0517 and CVE-2024-0518, in the V8 engine, enabling arbitrary code execution on compromised devices. The company has not disclosed specific details about the zero-day exploits used in attacks but may restrict access to bug details until a majority of users have received the fix.

#4

In the previous year, Google dealt with multiple Chrome zero-day vulnerabilities ([CVE-2023-2033](#), [CVE-2023-2136](#), [CVE-2023-3079](#), [CVE-2023-4863](#), [CVE-2023-5217](#), [CVE-2023-6345](#) and [CVE-2023-7024](#)) highlighting the imperative to bolster the browser's security.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-0519	Google Chrome prior to 120.0.6099.224	cpe:2.3:a:google:chrome: *:*:*:*:*:*	CWE-125
CVE-2024-0518	Google Chrome prior to 120.0.6099.224	cpe:2.3:a:google:chrome: *:*:*:*:*:*	CWE-843
CVE-2024-0517	Google Chrome prior to 120.0.6099.224	cpe:2.3:a:google:chrome: *:*:*:*:*:*	CWE-787

Recommendations



Update Chrome: Ensure that Google Chrome is updated to the latest versions 120.0.6099.224/225 for Windows, 120.0.6099.234 for Mac, and 120.0.6099.224 for Linux. Open Chrome, go to "Settings," scroll down to "About Chrome," and allow the browser to check for updates.



Regular Software Updates: Keep all software, including the operating system and security software, up-to-date. Regular updates often include patches for known vulnerabilities.



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



Vulnerability Management: This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.

Potential MITRE ATT&CK TTPs

<u>TA0002</u> Execution	<u>TA0042</u> Resource Development	<u>TA0007</u> Discovery	<u>T1059</u> Command and Scripting Interpreter
<u>T1082</u> System Information Discovery	<u>T1588</u> Obtain Capabilities	<u>T1588.005</u> Exploits	<u>T1588.006</u> Vulnerabilities

Patch Links

Update Chrome browser to the latest version 120.0.6099.224/225 for Windows, 120.0.6099.234 for Mac, and 120.0.6099.224 for Linux.

Links:

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

References

https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_16.html

<https://chromereleases.googleblog.com/>

<https://www.hivepro.com/threat-advisory/googles-battle-against-zero-day-vulnerability-continues/>

<https://www.hivepro.com/threat-advisory/apple-addresses-zero-day-flaws-exploited-in-the-wild/>

<https://www.hivepro.com/threat-advisory/google-chrome-emergency-update-fixes-zero-day-exploit-in-the-wild/>

<https://www.hivepro.com/threat-digest/cisa-known-exploited-vulnerability-catalog-april-2023/>

<https://www.hivepro.com/threat-advisory/google-addresses-high-stakes-chrome-zero-day-vulnerability/>

<https://www.hivepro.com/threat-advisory/google-addresses-fourth-zero-day-flaw-exploited-by-attackers-wildly/>

<https://www.hivepro.com/threat-advisory/google-and-firefox-fixes-zero-day-flaw-exploited-in-the-wild/>

<https://www.hivepro.com/threat-advisory/google-addresses-sixth-zero-day-flaw-exploited-by-attackers-wildly/>

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

January 17, 2024 • 4:30 AM

© 2024 All Rights are Reserved by Hive Pro[®]



More at www.hivepro.com