

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Google and Firefox fixes Zero-Day Flaw Exploited in the Wild

Date of Publication

September 29, 2023

Last Update Date

October 5, 2023

Admiralty Code

A1

TA Number

TA2023392

Summary

First Seen: September 25, 2023

Affected Products: Google Chrome, Firefox, Firefox ESR, Firefox Focus for Android, Firefox for Android

Affected Platform: Windows, Mac and Linux

Impact: A zero-day vulnerability, CVE-2023-5217, is actively exploited and has been patched in both Google Chrome and Firefox browsers. CVE-2023-5217 is a Heap buffer overflow vulnerability discovered in the vp8 encoding component of libvpx, which has the potential to allow the execution of arbitrary code on the targeted system. Additionally, Google addressed multiple security issues including CVE-2023-5186 and CVE-2023-5187. Both CVE-2023-5186 and CVE-2023-5187 are use-after-free flaws and they could also lead to arbitrary code execution.

⚙️ CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-5217	Google Chrome libvpx Heap Buffer Overflow Vulnerability	Google Chrome, Firefox, Firefox ESR, Firefox Focus for Android, Firefox for Android	✓	✓	✓
CVE-2023-5186	Google Chrome Use after free in Passwords Vulnerability	Google Chrome	✗	✗	✓
CVE-2023-5187	Google Chrome Use after free in Extensions Vulnerability	Google Chrome	✗	✗	✓

Vulnerability Details

#1

A recently discovered zero-day vulnerability, CVE-2023-5217, is actively exploited in the wild and has been patched in both Google Chrome and Firefox browsers. CVE-2023-5217 is categorized as a zero-day vulnerability, specifically a heap-based buffer overflow within the VP8 compression format in the libvpx library. Google has also taken steps to address several security issues in Google Chrome for Desktop, including high-severity vulnerabilities like CVE-2023-5186 and CVE-2023-5187.

#2

The CVE-2023-5217 vulnerability poses a risk of remote system compromise. It originates from a boundary error that arises while processing untrusted HTML content in the vp8 encoding component within libvpx. A remote attacker can exploit this vulnerability by creating a malicious web page, tricking the victim into visiting it. The attacker can then trigger a heap-based buffer overflow, potentially executing arbitrary code on the victim's system.


#3


CVE-2023-5186 is a vulnerability stemming from a use-after-free error in Google Chrome's Passwords component, while CVE-2023-5187 is another vulnerability resulting from a use-after-free error, but in the Extensions component of Google Chrome. In both cases, an attacker can exploit these flaws by enticing the victim to visit a malicious web page, thereby triggering the use-after-free error and potentially executing arbitrary code on the victim's system. Both vulnerabilities have the potential to allow an attacker to compromise the affected system, leading to unauthorized access and control.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-5217	Google Chrome: 100.0.4896.60 - 117.0.5938.92, Firefox 100.0 - 118.0, Firefox ESR 10.0 - 115.3.0, Firefox Focus for Android 108.2.0 - 118.0, Firefox for Android 66.0.4 - 118.0	cpe:2.3:a:webmproject:libvpx:1. 13.1:*:*:*:*:* cpe:2.3:a:google:chrome:*:*:*:* *:*:* cpe:2.3:a:mozilla:firefox:*:*:*:* *:*:* cpe:2.3:a:mozilla:firefox:*:*:*:* *:android:*:* cpe:2.3:a:mozilla:firefox_esr:*:* *:*:*:* cpe:2.3:a:mozilla:firefox_focus:* *:*:*:*:android:*:*	CWE-787
CVE-2023-5186	Google Chrome: 100.0.4896.60 - 117.0.5938.92	cpe:2.3:a:google:chrome:*:*:*:* *:*:*	CWE-416
CVE-2023-5187	Google Chrome: 100.0.4896.60 - 117.0.5938.92	cpe:2.3:a:google:chrome:*:*:*:* *:*:*	CWE-416

Recommendations

 **Apply Patch:** Google and Mozilla have released updates to address these vulnerabilities. Make sure to update your browser to the **fixed version**.

 **Browser Security:** Customize your browser's privacy settings according to your preferences and consider using browser extensions that enhance security and privacy. Ensure your browser is always up to date and restrict the use of plugins and extensions to essential ones. Additionally, verify websites for HTTPS protection and avoid visiting unsolicited websites.

Potential MITRE ATT&CK TTPs

<u>TA0001</u> Initial Access	<u>TA0002</u> Execution	<u>TA0011</u> Command and Control	<u>TA0005</u> Defense Evasion
<u>TA0007</u> Discovery	<u>TA0042</u> Resource Development	<u>T1055</u> Process Injection	<u>T1082</u> System Information Discovery
<u>T1569</u> System Services	<u>T1078</u> Valid Accounts	<u>T1105</u> Ingress Tool Transfer	<u>T1087</u> Account Discovery
<u>T1588</u> Obtain Capabilities	<u>T1588.006</u> Vulnerabilities	<u>T1033</u> System Owner/User Discovery	<u>T1189</u> Drive-by Compromise
<u>T1566</u> Phishing			

Patch Details

Ensure that your Google Chrome is updated to at least version 117.0.5938.132. This update addresses multiple security issues including CVE-2023-5217, CVE-2023-5186, and CVE-2023-5187.

Link:

https://chromereleases.googleblog.com/2023/09/stable-channel-update-for-desktop_27.html

Ensure that Firefox is updated to at least version 118.0.1, Firefox ESR (Extended Support Release) to version 115.3.1, Firefox Focus for Android to version 118.1 and Firefox for Android to version 118.1.

Link:

<https://www.mozilla.org/en-US/security/advisories/mfsa2023-44/>

References

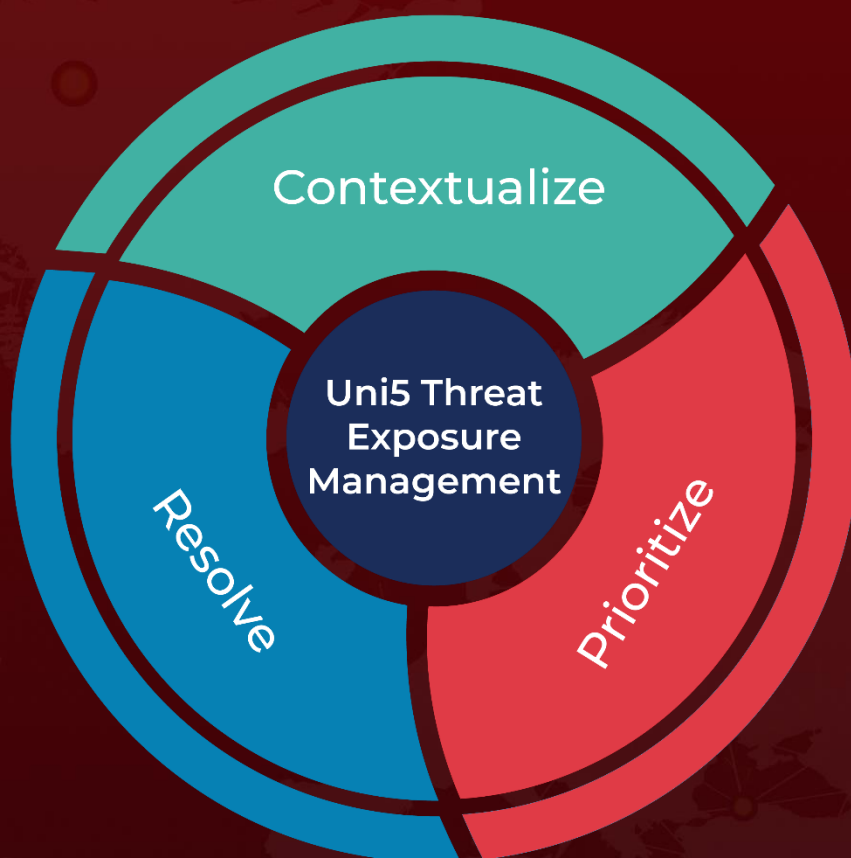
https://chromereleases.googleblog.com/2023/09/stable-channel-update-for-desktop_27.html

<https://www.mozilla.org/en-US/security/advisories/mfsa2023-44/>

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

September 29, 2023 • 7:30 AM

© 2023 All Rights are Reserved by HivePro®



More at www.hivepro.com