HiveForce Labs
THREAT ADVISORY

🐛 VULNERABILITY REPORT

Google Addresses Sixth Zero-Day Flaw Exploited by Attackers Wildly

Summary

First Seen: November 24, 2023
Affected Product: Google Chrome
Affected Platform: Windows, Linux, macOS
Impact: Multiple vulnerabilities have been discovered in Google Chrome, including a zero-day vulnerability (CVE-2023-6345) actively exploited for remote code execution. Users are advised to update Chrome to versions 119.0.6045.199/.200 (Windows) or 119.0.6045.199 (Mac and Linux) promptly to safeguard against the identified vulnerabilities.

⚙ CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-6345	Google Chrome Skia Integer Overflow Vulnerability	Google Chrome	✅	✅	✅
CVE-2023-6347	Google Chrome Mojo Use After Free Vulnerability	Google Chrome	❌	❌	✅
CVE-2023-6346	Google Chrome WebAudio Use After Free Vulnerability	Google Chrome	❌	❌	✅
CVE-2023-6350	Google Chrome Libavif Out-of-Bounds Vulnerability	Google Chrome	❌	❌	✅
CVE-2023-6351	Google Chrome Libavif Use After Free Vulnerability	Google Chrome	❌	❌	✅
CVE-2023-6348	Google Chrome Spellcheck Type Confusion Vulnerability	Google Chrome	❌	❌	✅

Vulnerability Details

#1 Google has urgently released a critical security update for its Chrome browser to address a zero-day vulnerability (CVE-2023-6345) that is actively exploited. The flaw, discovered by Google's Threat Analysis Group, is related to an integer overflow issue in the Skia 2D graphics library used by Chrome, enabling attackers to remotely execute code on affected devices. The company has confirmed the existence of an exploit in the wild, emphasizing the need for users to promptly update their browsers.

#2 Alongside the zero-day fix, Google addressed six other security issues in the latest Chrome update, including type confusion, use-after-free, and out-of-bounds memory access vulnerabilities. Users are advised to update Chrome to version 119.0.6045.199/.200 for Windows and 119.0.6045.199 for Mac and Linux to safeguard against the vulnerabilities. In September, Google had addressed two other zero-days CVE-2023-5217 and CVE-2023-4863, and this marks the sixth Chrome zero-day fixed in 2023.

⚛ Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-6348			CWE-843
CVE-2023-6347			CWE-416
CVE-2023-6346	Google Chrome: 100.0.4896.60 - 119.0.6045.160	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	CWE-416
CVE-2023-6350			CWE-119
CVE-2023-6351			CWE-416
CVE-2023-6345			CWE-190

Recommendations

Update Google Chrome: Ensure your Chrome browser is updated to the latest version (119.0.6045.199/.200 for Windows and 119.0.6045.199 for Mac and Linux). Open Chrome, go to "Settings," scroll down to "About Chrome," and allow the browser to check for updates.

Keep Operating System Updated: Regularly update your operating system (Windows, macOS, or Linux) to apply the latest security patches and improvements.

Use Security Software: Employ reputable antivirus and anti-malware software to add an extra layer of protection against potential threats.

⚛ Potential MITRE ATT&CK TTPs

TA0002	TA0001	TA0040	TA0042
Execution	Initial Access	Impact	Resource Development
T1059	**T1203**	**T1588.005**	**T1588**
Command and Scripting Interpreter	Exploitation for Client Execution	Exploits	Obtain Capabilities
T1588.006			
Vulnerabilities			

Patch Details

Update Chrome browser to the latest version 119.0.6045.199/.200 for Windows and 119.0.6045.199 for Mac and Linux

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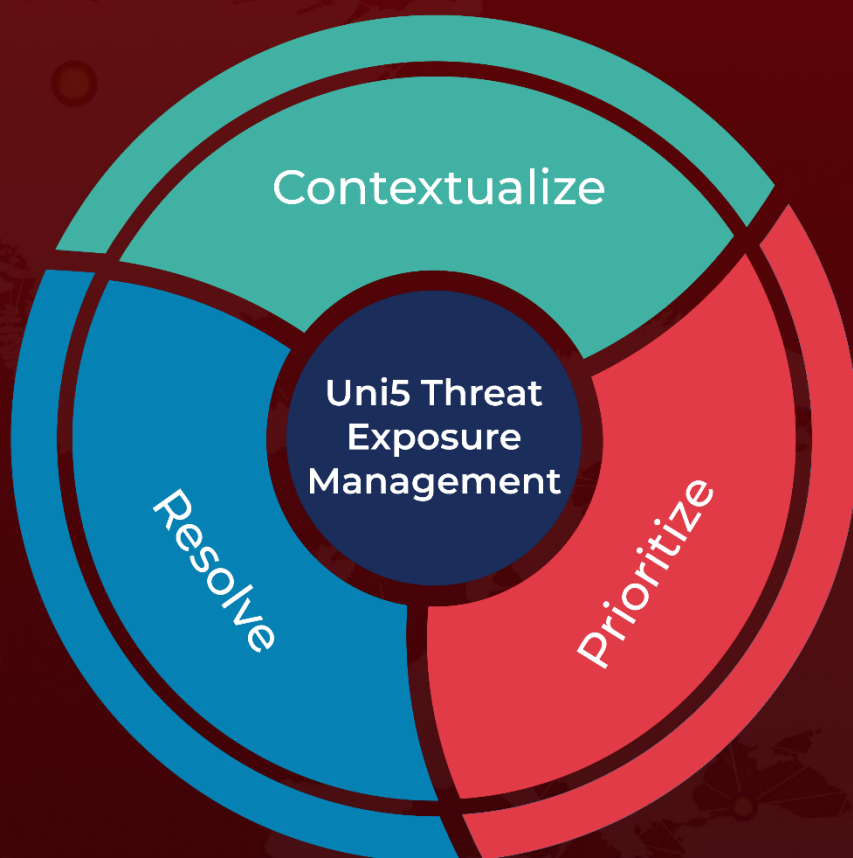https://www.google.com/intl/en/chrome/?standalone=1

References

https://chromereleases.googleblog.com/2023/11/stable-channel-update-for-desktop_28.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.