Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Google Patches High-Risk V8 Zero-Day Hitting Chrome Users

Date of Publication	Admiralty Code	TA Number
November 18, 2025	A1	TA2025350

Summary

First Seen: November 2025
Affected Products: Google Chrome
Impact: Google has issued an urgent security update for Chrome after discovering a zero-day vulnerability in the V8 engine that attackers are already exploiting in the wild. The flaw, tracked as CVE-2025-13223, allows malicious websites to corrupt memory and potentially run code on a victim's device without any interaction. Users are strongly encouraged to update Chrome to the latest version across Windows, macOS, and Linux to stay protected from these active threats.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-13223	Google Chromium V8 Type Confusion Vulnerability	Google Chrome	✓	✗	✓

Vulnerability Details

#1

Google has rolled out an urgent set of security updates for its Chrome browser, addressing multiple vulnerabilities, including a zero-day that attackers are already exploiting in real-world attacks. The actively abused flaw, tracked as CVE-2025-13223, is a type confusion bug in the V8 JavaScript engine. This issue could allow a remote attacker to trigger heap corruption simply by getting a user to load a maliciously crafted HTML page, opening the door to potential code execution.

#2 Google has confirmed that an exploit for this vulnerability is circulating in the wild, meaning attackers may be able to execute arbitrary code on targeted devices without requiring any user interaction. Given its active exploitation status, the risk associated with this flaw is significantly elevated. Alongside the zero-day, Google also fixed a second V8 type confusion issue, CVE-2025-13224, as part of the same patch cycle. While this one is not known to be exploited, it still poses a risk if left unpatched.

#3 To stay protected, users should update Google Chrome to the latest secure builds: 142.0.7444.175/.176 on Windows, 142.0.7444.176 on macOS, and 142.0.7444.175 on Linux. You can verify and apply updates by navigating to More > Help > About Google Chrome, allowing the browser to check for new versions, and selecting Relaunch to complete the process. Keeping Chrome up to date is the most effective way to stay ahead of active threats like this zero-day.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-13223	Google Chrome prior to 142.0.7444.175	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	CWE-843

Recommendations

Update Chrome Immediately: Install the latest version of Google Chrome on your device to ensure you're protected from the actively exploited zero-day.

Enable Automatic Updates: Let Chrome handle updates in the background so you're always running the safest version.

Be Cautious with Unfamiliar Websites or Links: Since the exploit can be triggered through crafted HTML pages, avoid clicking on suspicious links or visiting untrusted sites.

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

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

Patch Details

Upgrade Google Chrome to version 142.0.7444.175/.176 on Windows, 142.0.7444.176 on macOS, and 142.0.7444.175 on Linux.

Link:
https://chromereleases.googleblog.com/2025/11/stable-channel-update-for-desktop_17.html

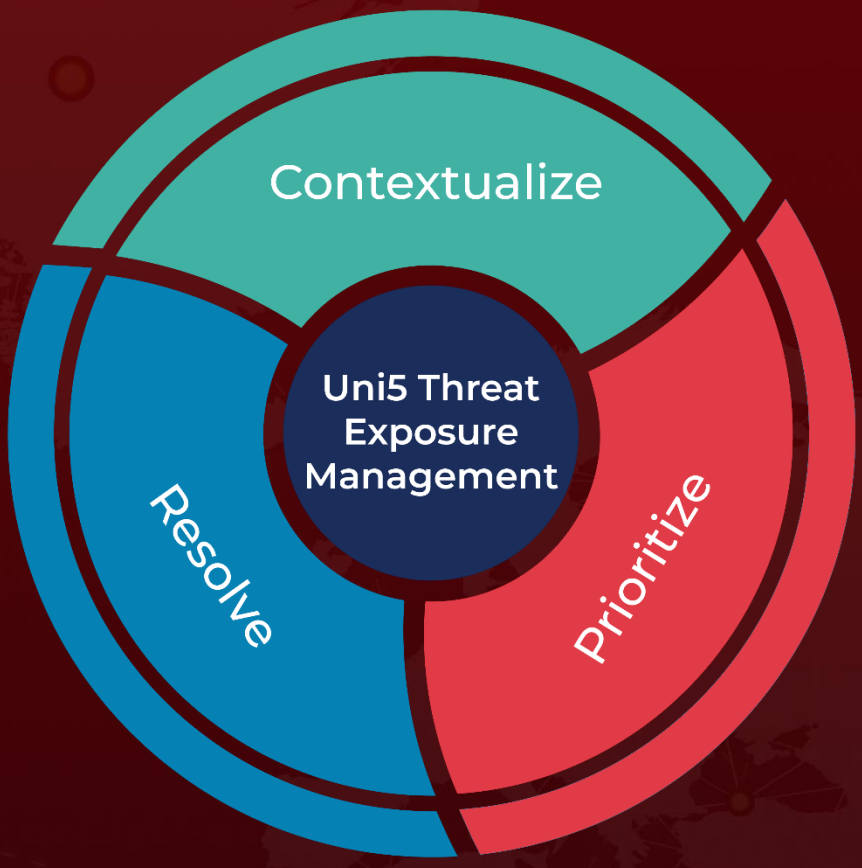
References

https://chromereleases.googleblog.com/2025/11/stable-channel-update-for-desktop_17.html?m=1

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

November 18, 2025 . 9:00 AM

More at www.hivepro.com