Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Google Races to Patch Chrome's Sixth Zero-Day CVE-2025-10585

Date of Publication	Admiralty Code	TA Number
September 19, 2025	A1	TA2025290

Summary

Discovered On: September 16, 2025
Affected Products: Google Chrome (and all Chromium-based browsers)
Affected OS: Windows, Mac, Linux,
Impact: Google has released critical security updates for Chrome to fix its sixth zero-day vulnerability of 2025, identified as CVE-2025-10585. The flaw is a type confusion issue in the V8 JavaScript engine, which is already being actively exploited. If left unpatched, it could allow attackers to crash systems or execute malicious code. Users of Chromium-based browsers are strongly urged to update without delay.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-10585	Google Chromium V8 Type Confusion Vulnerability	Google Chrome (Chromium-based browsers)	✓	✗	✓

Vulnerability Details

#1 Google has released security updates for its Chrome web browser to address its sixth zero-day vulnerability of 2025. Tracked as CVE-2025-10585, the flaw is a type confusion issue in Chrome's V8 JavaScript and WebAssembly engine, and it has already been exploited in the wild. The update also addresses three other high-severity vulnerabilities, including use-after-free flaws in Dawn and WebRTC, as well as a heap buffer overflow in ANGLE.

#2 This vulnerability stems from type confusion in V8, Chrome's underlying JavaScript engine. Exploiting it could allow attackers to disrupt the browser or the host system, potentially enabling the execution of arbitrary code. Type confusion flaws are particularly dangerous, as they can be weaponized to cause unexpected software behavior, program crashes, and unauthorized code execution.

#3

CVE-2025-10585 is the latest in a series of zero-day vulnerabilities affecting Chrome this year. Previous cases include CVE-2025-2783, CVE-2025-4664, CVE-2025-5419, CVE-2025-6554, and CVE-2025-6558, all of which were either actively exploited or demonstrated as proof-of-concept attacks.

#4

The security fix is available in Chrome version 140.0.7339.185/.186 for Windows and Mac, and 140.0.7339.185 for Linux. Users are strongly advised to update immediately by navigating to Chrome's settings menu, selecting "About Google Chrome," and allowing the browser to perform an automatic update check.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-10585	Google Chrome prior to 140.0.7339.185	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	CWE-843

Recommendations

Install Chrome Updates Without Delay: Upgrade to version 140.0.7339.185/.186 on Windows and macOS or 140.0.7339.185 on Linux to ensure protection against the vulnerability. Navigate to 'About Google Chrome' to verify that the latest version is installed, then select Relaunch to activate the update. After the update has been downloaded, restart Chrome promptly. Open tabs will be restored automatically, with the exception of Incognito tabs, which will not reopen.

Enable Site Isolation in Chrome: Site Isolation ensures each website runs in a separate renderer process, preventing them from sharing memory. This limits the impact of memory corruption flaws such as type confusion, which attackers exploit to manipulate memory and execute malicious code. Enabling Strict Site Isolation (chrome://flags/#enable-site-per-process) helps contain potential attacks, preventing compromised sites from accessing data or processes belonging to others. Although it may slightly increase memory usage, the security benefits outweigh the trade-off, making it especially important for enterprise systems, sensitive environments, and high-risk users like administrators and developers.

Enable Automatic Updates Enterprise-Wide: For organizations, enforce automatic update policies using Group Policy (Windows) or configuration profiles (macOS/Linux) to ensure timely patching across all systems. System administrators should inventory and monitor browser versions within the environment using endpoint management tools to identify outdated instances.

Vulnerability Management: This entails systematically identifying, assessing, and remediating software vulnerabilities through timely updates and patching. Organizations should maintain a comprehensive inventory of software versions and applied security fixes, while also reviewing the security posture of third-party vendors, particularly those providing critical applications and services.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0004** Privilege Escalation
TA0008 Lateral Movement	**TA0042** Resource Development	**T1588** Obtain Capabilities	**T1189** Drive-by Compromise
T1203 Exploitation for Client Execution	**T1204** User Execution	**T1210** Exploitation of Remote Services	**T1068** Exploitation for Privilege Escalation
T1059 Command and Scripting Interpreter	**T1588.006** Vulnerabilities		

Patch Details

Upgrade to 140.0.7339.185/.186 for Windows/Mac, and 140.0.7339.185 for Linux, which will roll out over the coming days/weeks.

Links:
https://chromereleases.googleblog.com/2025/09/stable-channel-update-for-desktop_17.html

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

References

https://chromereleases.googleblog.com/2025/09/stable-channel-update-for-desktop_17.html

https://hivepro.com/threat-advisory/chrome-zero-day-exploited-in-operation-forumtroll/

https://hivepro.com/threat-advisory/cve-2025-4664-google-chromes-zero-day-flaw-exploited-in-the-wild/

https://hivepro.com/threat-advisory/google-rushes-to-fix-chrome-zero-day-vulnerability/

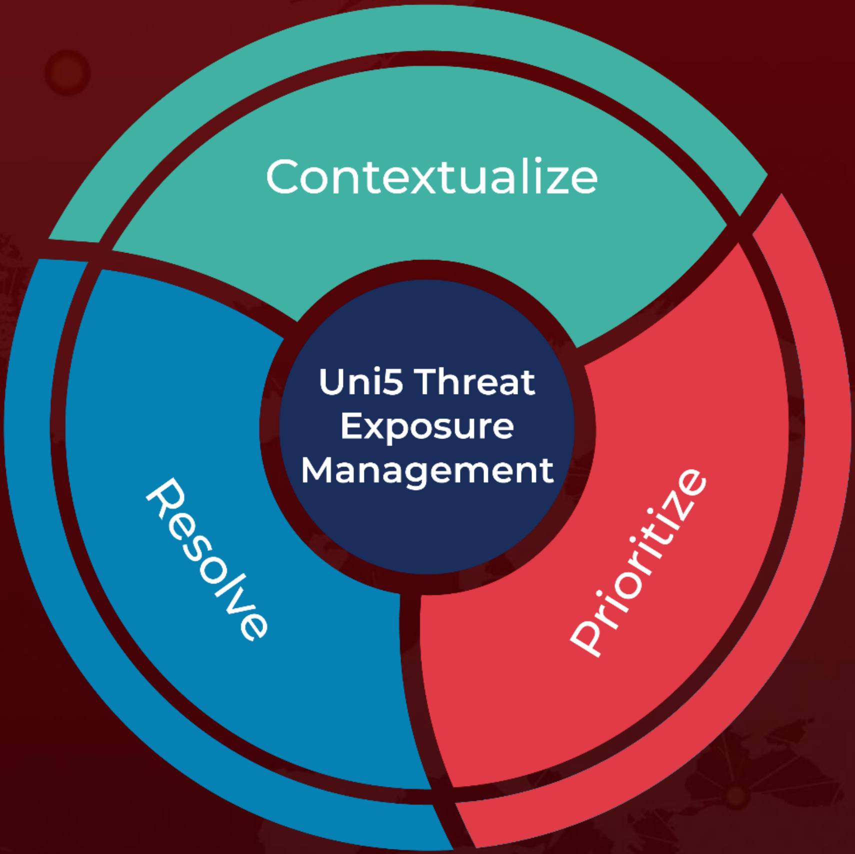
https://hivepro.com/threat-advisory/cve-2025-6554-google-chromes-zero-day-flaw-exploited-in-the-wild/

https://hivepro.com/threat-advisory/cve-2025-6558-chrome-flaw-lets-hackers-break-the-sandbox/

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 19, 2025 • 9:30 AM

© 2025 All Rights are Reserved by Hive Pro

More at www.hivepro.com