Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

CVE-2025-6554: Google Chrome’s Zero-Day Flaw Exploited in the Wild

Date of Publication	Admiralty Code	TA Number
July 2, 2025	A1	TA2025203

Summary

First Seen: June 25, 2025
Affected Product: Google Chrome (and all Chromium-based browsers)
Impact: CVE-2025-6554 is a critical zero-day type confusion vulnerability in Google's V8 JavaScript engine affecting Chrome versions prior to 138.0.7204.96. The flaw allows attackers to corrupt memory and execute arbitrary code within the browser context, enabling full browser compromise. Successful exploitation could lead to sandbox escape and remote code execution on the host system. Google confirmed active in-the-wild exploitation before the public patch release. Users are strongly advised to update Chrome and other Chromium-based browsers immediately to prevent compromise.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-6554	Google Chromium V8 Type Confusion Vulnerability	Google Chrome	✓	✗	✓

Vulnerability Details

#1

CVE-2025-6554 is a critical, actively exploited zero-day vulnerability in the V8 JavaScript engine used by Google Chrome and other Chromium-based browsers. The flaw is rooted in a type confusion issue, where the engine may incorrectly assume the type of a JavaScript object during execution. This allows attackers to craft malicious JavaScript that causes V8 to treat one object type as another, leading to out-of-bounds memory access. As a result, attackers can achieve arbitrary read and write capabilities in the browser's memory, which can be escalated to remote code execution (RCE) within the browser context.

#2

This vulnerability is particularly dangerous because exploitation requires nothing more than visiting a malicious or compromised website, no additional user interaction is necessary. Once exploited, attackers can execute arbitrary code, inject payloads into memory, or potentially gain persistence and move laterally, especially if they chain this flaw with a sandbox escape or privilege escalation vulnerability.

#3

The underlying cause of such vulnerabilities in V8 often relates to Just-In-Time (JIT) compiler optimizations. When assumptions about JavaScript object structures are violated, such as by dynamically altering an object's shape during execution, the engine may skip critical type checks, resulting in type confusion. This has been a recurring attack vector in Chrome's security history due to the complexity and performance demands of modern JIT engines. Furthermore, exploits leveraging this bug are difficult for traditional antivirus or endpoint detection solutions to catch, as the attack can be delivered and executed entirely in memory.

#4

Google issued emergency patches for Chrome (version 138.0.7204.96+ on Windows/Linux and 138.0.7204.92+ on macOS) shortly after confirming in-the-wild exploitation. Users and organizations are strongly urged to update all Chromium-based browsers immediately and remain vigilant, as technical details are being withheld until a majority of users are protected, and further exploitation attempts are likely.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-6554	Google Chrome prior to 138.0.7204.96	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	CWE-843

Recommendations

Update Google Chrome Immediately: All users and administrators should ensure Chrome is updated to version 138.0.7204.96 or later on Windows and Linux, and 138.0.7204.92 or later on macOS. These versions contain the official patch for CVE-2025-6554. Updates can be applied manually by navigating to chrome://settings/help, or automatically if enterprise policies permit. Chromium-based browsers such as Microsoft Edge, Brave, and Opera should also be updated to their latest versions as soon as corresponding patches are released.

Enable Browser Hardening Features: To reduce the attack surface for future exploitation attempts, enable security-enhancing browser settings. These include Site Isolation (chrome://flags/#enable-site-per-process) and Enhanced Safe Browsing. Enterprise administrators can enforce these settings via group policy to ensure uniform protection across user endpoints.

Restrict JavaScript Execution in High-Risk Environments: For users in sensitive roles (e.g., executives, journalists, system administrators), consider deploying browser extensions that restrict JavaScript execution on untrusted domains (e.g., NoScript). Additionally, configure DNS and firewall policies to block known malicious JavaScript CDN domains and prevent access to known exploit-hosting infrastructure.

Enhance Browser Security: Use enterprise-grade browser security tools to strengthen sandboxing and prevent attackers from bypassing isolation layers. Implement behavioral-based monitoring to detect unusual browser activity, such as unauthorized privilege escalations or unexpected process injections.

Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0042** Resource Development	**TA0001** Initial Access	**TA0004** Privilege Escalation
T1189 Drive-by Compromise	**T1203** Exploitation for Client Execution	**T1059.007** JavaScript	**T1059** Command and Scripting Interpreter
T1068 Exploitation for Privilege Escalation	**T1588** Obtain Capabilities	**T1588.005** Exploits	**T1588.006** Vulnerabilities

Patch Details

Upgrade Google Chrome version to 138.0.7204.96 (Windows/Linux) and 138.0.7204.92 (macOS) or latest version.

Link:
https://chromereleases.googleblog.com/2025/06/stable-channel-update-for-desktop_30.html

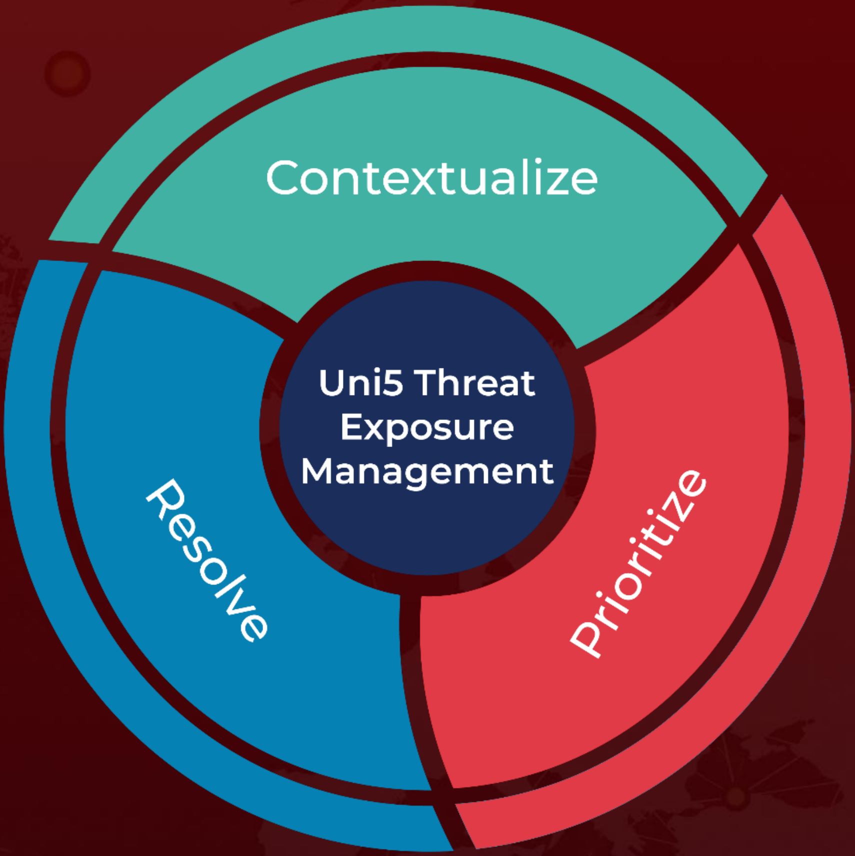
References

https://threatprotect.qualys.com/2025/07/01/google-addresses-zero-day-vulnerability-impacting-chrome-browser-cve-2025-6554/

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

July 2, 2025 • 4:30 AM

More at www.hivepro.com