CVE-2025-6554: TYPE CONFUSION IN V8 IN GOOGLE CHROME

Vairav CVE Report

Date: July 01, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

Google has released an urgent security update for the Chrome browser to address a high-severity zero-day vulnerability (CVE-2025-6554) that is actively exploited in the wild. The vulnerability, caused by a type confusion flaw in the V8 JavaScript engine, could allow remote attackers to execute arbitrary code on targeted systems. Chrome has been updated to version 138.0.7204.96/.97 (Windows), 138.0.7204.92/.93 (Mac), and 138.0.7204.96 (Linux) to mitigate the issue. All users are strongly advised to update immediately.

VULNERABILITY DETAILS

CVE-2025-6554: Type Confusion in V8 JavaScript Engine

Description: This vulnerability involves a type confusion issue in Chrome's V8 JavaScript engine, which occurs when the browser misinterprets an object type during execution. This allows an attacker to manipulate memory, potentially executing arbitrary code within the browser context. The flaw can be exploited via a specially crafted HTML page.

Impact: Remote Code Execution

CVSS Score: Not officially published; rated High by Google

Exploit Status: Confirmed exploitation in the wild

AFFECTED PRODUCTS/VERSIONS

- Chrome versions prior to 138.0.7204.96 (Linux)
- Chrome versions prior to 138.0.7204.96/.97 (Windows)
- Chrome versions prior to 138.0.7204.92/.93 (Mac)

EXPLOIT DETAILS

Google has confirmed that CVE-2025-6554 is being actively exploited in the wild. The flaw allows remote attackers to achieve arbitrary code execution via type confusion, potentially resulting in system compromise. Exploitation can occur through a maliciously crafted webpage and does not require user interaction beyond visiting the page.

RECOMMENDED ACTIONS

- **Update Immediately:** Upgrade Chrome to version 138.0.7204.96/.97 (Windows), 138.0.7204.92/.93 (Mac), or 138.0.7204.96 (Linux).

- **Verify Installation:** Go to chrome://settings/help to trigger and verify the update.
- **Restart Chrome:** Restart the browser to apply the patch after updating.
- **Enterprise Rollout:** Organizations should prioritize patch deployment to prevent potential compromise on scale.

REFERENCES

https://cybersecuritynews.com/chrome-0-day-vulnerability-exploited/

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

https://www.cve.org/CVERecord?id=CVE-2025-6554

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com