GOOGLE CHROME FIXES TWO HIGH-SEVERITY RCE VULNERABILITIES (CVE-2025-5958 & CVE-2025-5959)

Vairav CVE Report

Date: June 11, 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 a new Stable Channel update for Chrome Desktop (version 137.0.7151.103/.104 for Windows and macOS, 137.0.7151.103 for Linux), addressing two high-severity vulnerabilities, CVE-2025-5958 and CVE-2025-5959. These Media and V8 components' flaws could allow remote attackers to execute arbitrary code through use-after-free and type confusion exploitation techniques. Google urges all users to apply the update promptly as the rollout proceeds over the coming days.

VULNERABILITY DETAILS

CVE-2025-5958: Use-After-Free in Media

Description: A use-after-free vulnerability in Chrome's Media component, triggered when a media object is accessed after being freed from memory. Exploiting this flaw could enable attackers to execute arbitrary code through a crafted HTML page.

Impact: Remote Code Execution

CVSS Score: High

CVE-2025-5959: Type Confusion in V8

Description: A type confusion flaw in Chrome's V8 JavaScript engine. If successfully exploited, it could allow attackers to manipulate memory, potentially leading to sandbox escapes or arbitrary code execution.

Impact: Remote Code Execution / Sandbox Escape

CVSS Score: High

AFFECTED PRODUCTS/VERSIONS

- Chrome versions prior to 137.0.7151.103 (Linux)
- Chrome versions prior to 137.0.7151.103/.104 (Windows, macOS)

EXPLOIT DETAILS

As part of its standard practice, Google has limited public access to technical information on these vulnerabilities to prevent potential misuse. No known public exploits have been reported as of the time of this update.

RECOMMENDATIONS

- Ensure Chrome Desktop is updated to version 137.0.7151.103/.104.
- Visit chrome://settings/help to manually trigger the update and confirm patching.
- Use endpoint protection tools to watch for any suspicious browser activities.
- Edge, Brave, Opera, and others should also apply updates as they become available.

REFERENCES

https://www.cve.org/CVERecord?id=CVE-2025-5958

https://www.cve.org/CVERecord?id=CVE-2025-5959

https://securityonline.info/chrome-update-alert-two-high-severity-flaws-patched-update-now-to-stay-safe/

https://chromereleases.googleblog.com/2025/06/stable-channel-update-for-desktop_10.html

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