



CHROME ZERO-DAY EXPLOITED IN THE WILD: CRITICAL RCE VULNERABILITY PATCHED

Vairav CVE Report

Date: June 03, 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 out-of-band update for its Chrome browser to address a critical zero-day vulnerability (CVE-2025-5419) that is being exploited in the wild. The flaw exists in the V8 JavaScript engine and could allow remote attackers to cause heap corruption and execute arbitrary code. Another medium-severity vulnerability (CVE-2025-5068) was also patched in this update. Users are strongly advised to update to Chrome version 137.0.7151.68/.69 for Windows and macOS, and 137.0.7151.68 for Linux to mitigate these threats.

VULNERABILITY DETAILS

CVE-2025-5419: Out-of-Bounds Read and Write in V8

Description: An out-of-bound read causes this vulnerability and write issue in the V8 JavaScript and WebAssembly engine. A remote attacker can exploit this flaw using a specially crafted HTML page, potentially causing heap corruption and enabling remote code execution.

Impact: Remote Code Execution

CVSS Score: 8.8 (High)

CVE-2025-5068: Use-After-Free in Blink

Description: A use-after-free vulnerability in the Blink rendering engine. Exploitation of this flaw could lead to arbitrary code execution.

Impact: Remote Code Execution

CVSS Score: Medium

AFFECTED PRODUCTS/VERSIONS

- Chrome prior to 137.0.7151.68 (Linux)
- Chrome prior to 137.0.7151.68/.69 (Windows, macOS)

EXPLOIT DETAILS

CVE-2025-5419 is being actively exploited in the wild. Google has limited public details to prevent further abuse until most users have updated their systems. The vulnerability was mitigated via a configuration change pushed to the stable version on May 28, 2025.

RECOMMENDATIONS

- Upgrade Chrome to version 137.0.7151.68/.69 (Windows/macOS) or 137.0.7151.68 (Linux).
- Watch suspicious behavior and review threat detection logs.
- Users of Edge, Brave, Opera, and Vivaldi should also apply patches as they become available

REFERENCES

<https://thehackernews.com/2025/06/new-chrome-zero-day-actively-exploited.html>

<https://nvd.nist.gov/vuln/detail/CVE-2025-5419>

<https://chromereleases.googleblog.com/2025/06/stable-channel-update-for-desktop.html>

<https://nvd.nist.gov/vuln/detail/CVE-2025-5068>

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>