



CHROME SECURITY UPDATE FIXES VULNERABILITIES (CVE-2025-3619 & CVE-2025-3620)

Vairav CVE Report

Date: April 16, 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 critical security update for Chrome, version 135.0.7049.95/.96, addressing two severe vulnerabilities: a critical heap buffer overflow in Codecs and a high-severity use-after-free flaw in the USB subsystem. These vulnerabilities can allow remote attackers to execute arbitrary code and potentially take control of affected systems. Immediate patching is strongly advised to mitigate exploitation risks.

VULNERABILITY DETAILS

CVE-2025-3619: Heap Buffer Overflow in Codecs

Description: A critical heap buffer overflow vulnerability in the Codecs component of Google Chrome could allow remote attackers to execute arbitrary code. This flaw arises when the application writes more data to a buffer located on the heap than it can hold.

Impact: Remote Code Execution (RCE), system compromise.

CVSS Score: Critical

Exploitation: Successful exploitation could allow attackers to run malicious code on the target machine simply by convincing users to visit a specially crafted web page.

CVE-2025-3620: Use-After-Free in USB

Description: A use-after-free vulnerability in the USB subsystem of Chrome, occurs when memory is freed but still used, opening a window for attackers to exploit the dangling pointer.

Impact: Remote Code Execution (RCE), potential for full browser sandbox escape.

CVSS Score: High

Exploitation: Attackers could exploit this flaw by manipulating USB interactions, enabling arbitrary code execution via a crafted webpage or USB operation.

Affected Products and Versions:

- Google Chrome prior to 135.0.7049.95/.96 on Windows and macOS
- Google Chrome prior to 135.0.7049.95 on Linux

EXPLOIT DETAILS

Public technical details have been withheld by Google to prevent premature exploitation. There is no evidence of active exploitation in the wild currently. Google may delay disclosure further if third-party libraries are also affected and unpatched.

RECOMMENDATIONS

- Update Chrome immediately to version 135.0.7049.95/.96 via <chrome://settings/help>.
- Ensure automatic updates are enabled across enterprise systems.
- Monitor threat intelligence feeds for potential public exploits.
- Encourage user awareness of safe browsing habits to avoid phishing sites potentially designed to exploit these vulnerabilities.

REFERENCES

<https://securityonline.info/critical-chrome-security-update-patch-cve-2025-3619-cve-2025-3620-now/>

https://chromereleases.googleblog.com/2025/04/stable-channel-update-for-desktop_15.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>