



مجلس الأمن السيبراني  
CYBER SECURITY COUNCIL



**Security Updates – Google Chrome**

Tracking #:432317318

Date:28-05-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Google has released security updates to address multiple vulnerabilities in the Chrome browser.

## TECHNICAL DETAILS:

Google has released Chrome 137.0.7151.55/56 for Windows, Mac, and Linux, as well as Chrome 137.0.7151.51 for iOS. These vulnerabilities, if exploited, could allow remote attackers to execute arbitrary code, corrupt memory, bypass security restrictions, or cause denial of service (DoS).

### Vulnerability Details

- **CVE-2025-5063 (High Severity):** A use-after-free vulnerability in the Compositing component. Exploitation could allow an attacker to execute arbitrary code on the target system.
- **CVE-2025-5280 (High Severity):** An out-of-bounds write vulnerability in the V8 JavaScript engine. This flaw could lead to memory corruption and possible remote code execution.
- **CVE-2025-5064 (Medium Severity):** Inappropriate implementation in the Background Fetch API. This could expose user data or other sensitive information.
- **CVE-2025-5065 (Medium Severity):** An issue in the FileSystemAccess API related to inadequate validation. May lead to data exposure.
- **CVE-2025-5066 (Medium Severity):** A flaw in the Messages component that may enable spoofing or leakage of user communications.
- **CVE-2025-5281 (Medium Severity):** Inappropriate caching behavior in the Back/Forward Cache (BFCache) component, potentially bypassing security restrictions.
- **CVE-2025-5283 (Medium Severity):** A use-after-free vulnerability in libvpx, the video codec library. This could lead to memory corruption and potential application crashes or code execution.
- **CVE-2025-5067 (Low Severity):** Inappropriate implementation in the Tab Strip component, possibly allowing UI spoofing or misleading user interface behaviors.

### Fixed Versions:

- Stable Channel Update:
  - Chrome 137.0.7151.55/56 Windows and Mac
  - Chrome 137.0.7151.55 (Linux)
- Chrome Stable 137 (137.0.7151.51) for iOS

## RECOMMENDATIONS:

The UAE Cyber Security Council recommends to update Google Chrome to the latest version.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.



## REFERENCES:

- [https://chromereleases.googleblog.com/2025/05/stable-channel-update-for-desktop\\_27.html](https://chromereleases.googleblog.com/2025/05/stable-channel-update-for-desktop_27.html)
- <https://chromereleases.googleblog.com/>