



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Security Updates – Google Chrome

Tracking #:432319145

Date:17-06-2026

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 security updates to address multiple vulnerabilities in Google Chrome, including several critical use-after-free flaws and high-severity memory corruption, input validation, and security implementation issues. Successful exploitation of these vulnerabilities could allow attackers to execute arbitrary code, disclose sensitive information, bypass security controls, or cause browser crashes.

Vulnerability Details

Critical

- **CVE-2026-12437:** Use after free in WebShare
- **CVE-2026-12438:** Inappropriate implementation in WebView
- **CVE-2026-12439:** Use after free in Digital Credentials
- **CVE-2026-12440:** Use after free in DigitalCredentials
- **CVE-2026-12441:** Use after free in File Input
- **CVE-2026-12442:** Use after free in Passwords
- **CVE-2026-12443:** Use after free in Web Authentication

High

- **CVE-2026-12444:** Out of bounds read in Chromoting
- **CVE-2026-12445:** Use after free in Extensions
- **CVE-2026-12446:** Insufficient data validation in Passwords
- **CVE-2026-12447:** Heap buffer overflow in WebRTC
- **CVE-2026-12448:** Inappropriate implementation in WebView
- **CVE-2026-12449:** Use after free in Chromoting
- **CVE-2026-12450:** Inappropriate implementation in Media
- **CVE-2026-12451:** Use after free in DigitalCredentials
- **CVE-2026-12452:** Use after free in Downloads
- **CVE-2026-12453:** Insufficient validation of untrusted input in Input
- **CVE-2026-12454:** Race in Safe Browsing
- **CVE-2026-12455:** Use after free in Tab Strip
- **CVE-2026-12456:** Insufficient validation of untrusted input in Extensions
- **CVE-2026-12457:** Insufficient data validation in Extensions
- **CVE-2026-12458:** Incorrect security UI in Passwords
- **CVE-2026-12459:** Inappropriate implementation in Serial
- **CVE-2026-12460:** Insufficient policy enforcement in File System Access
- **CVE-2026-12461:** Out of bounds read in WebRTC
- **CVE-2026-12462:** Use after free in Media
- **CVE-2026-12463:** Inappropriate implementation in Views
- **CVE-2026-12464:** Use after free in Browser
- **CVE-2026-12465:** Insufficient validation of untrusted input in Metrics
- **CVE-2026-12466:** Heap buffer overflow in WebRTC
- **CVE-2026-12467:** Use after free in Extensions
- **CVE-2026-12468:** Inappropriate implementation in Updater
- **CVE-2026-12469:** Uninitialized Use in GPU

**Fixed Versions**

- Chrome Stable for Windows/Mac: 149.0.7827.155/.156 or later
- Chrome Stable for Linux: 149.0.7827.155 or later
- Chrome 149 (149.0.7827.159 or later) for Android

Additional Chrome updates:

- Chrome Extended Stable for Windows/Mac: 148.0.7778.271 or later

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/2026/06/stable-channel-update-for-desktop_01750511403.html
- <https://chromereleases.googleblog.com/>