

مجلس الأمن السيبراني  
CYBER SECURITY COUNCIL



**Security Updates – Google Chrome**

Tracking #:432318348

Date:04-02-2026

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 a security update for the Chrome browser to address multiple high-severity vulnerabilities that could be exploited to compromise system security.

### Vulnerability Details

- **CVE-2026-1861 (High):** Heap buffer overflow in *libvpx*, which could allow attackers to cause memory corruption through specially crafted media content.
- **CVE-2026-1862 (High):** Type confusion vulnerability in the *V8 JavaScript engine*, potentially enabling arbitrary code execution within the browser context.

### Impact

Successful exploitation of these vulnerabilities may allow remote attackers to execute arbitrary code, crash the browser, or compromise affected systems, particularly through malicious web content.

### Fixed Versions:

- Stable Channel Update for Desktop
  - Chrome 144.0.7559.132/.133 for Windows/Mac
  - Chrome 144.0.7559.132 for Linux
- Chrome 144 (144.0.7559.132) for Android

## 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/2026/02/stable-channel-update-for-desktop.html>
- <https://chromereleases.googleblog.com/>