



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Security Updates – Google Chrome

Tracking #:432318649

Date:24-03-2026

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:

A security update has been released by Google for the Google Chrome desktop browser, addressing eight high-severity vulnerabilities. The vulnerabilities primarily involve memory safety issues (use-after-free), heap buffer overflows, integer overflows, and out-of-bounds reads, which could potentially allow attackers to execute arbitrary code, cause browser crashes, or compromise system integrity.

High Severity Vulnerabilities

- CVE-2026-4673 – Heap buffer overflow in WebAudio
- CVE-2026-4674 – Out-of-bounds read in CSS
- CVE-2026-4675 – Heap buffer overflow in WebGL
- CVE-2026-4676 – Use-after-free in Dawn
- CVE-2026-4677 – Out-of-bounds read in WebAudio
- CVE-2026-4678 – Use-after-free in WebGPU
- CVE-2026-4679 – Integer overflow in Fonts
- CVE-2026-4680 – Use-after-free in FedCM

Fixed Versions:

- Stable Channel Update for Desktop
 - Chrome 146.0.7680.164 (Linux)
 - 146.0.7680.164/165Windows/Mac

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/>