مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Actively Exploited Zero-day Vulnerability in Google Chrome

Tracking #:432318403

Date:16-02-2026

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 INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Google has issued emergency security patches to remediate an actively exploited zero-day vulnerability.

TECHNICAL DETAILS:

Google has released an emergency security update for Chrome addressing CVE-2026-2441, a use-after-free vulnerability in the CSS rendering engine. Google has confirmed that exploits for this vulnerability are being actively used in attacks in the wild.

VULNERABILITY DETAILS

- CVE ID: **CVE-2026-2441**
- CVSS Severity: High
- Vulnerability Type: Use After Free (Memory Corruption)
- Attack Vector: Remote, via malicious web content
- User Interaction: Required (visiting malicious website)
- Privileges Required: None
- Exploit Status: ACTIVELY EXPLOITED IN THE WILD

Fixed Versions:

- Chrome 145.0.7632.75/76 for Windows/Mac
- Chrome 144.0.7559.75 for Linux

RECOMMENDATIONS:

- Update Chrome to the fixed or 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_13.html