مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates – Chrome OS

Tracking #:432318867

Date:30-04-2026

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

EXECUTIVE SUMMARY:

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

TECHNICAL DETAILS:

Google has released a Long Term Support (LTS) update for ChromeOS, addressing multiple security vulnerabilities affecting key browser and platform components. The update includes fixes for memory corruption and API-related flaws that could potentially be exploited for code execution or privilege abuse.

Vulnerability Details
Critical

- **CVE-2026-6297** – Use after free in Proxy

High

- **CVE-2026-4456** – Use after free in Digital Credentials API
- **CVE-2026-4680** – Use after free in FedCM
- **CVE-2026-4675** – Heap buffer overflow in WebGL

Fixed Versions

- LTS-144 version 144.0.7559.249 (Platform Version: 16503.81.0)

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the security updates recently released by Google for Chrome OS.

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/2026/04/long-term-support-channel-update-for_29.html