مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates – Chrome OS

Tracking #:432318943

Date:12-05-2026

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) channel update for ChromeOS, upgrading most supported devices to LTS-144 version 144.0.7559.250 (Platform Version 16503.82.0). The update addresses multiple high-severity vulnerabilities affecting key browser components, primarily related to use-after-free memory corruption issues that could potentially lead to system compromise or denial of service.

Vulnerability Details
High Severity

- CVE-2026-3921 — Use-after-free vulnerability in TextEncoding
- CVE-2026-5280 — Use-after-free vulnerability in WebCodecs
- CVE-2026-3923 — Use-after-free vulnerability in WebMIDI
- CVE-2026-4454 — Use-after-free vulnerability in Network components
- CVE-2026-5866 — Use-after-free vulnerability in Media
- CVE-2026-6303 — Use-after-free vulnerability in Codecs
- CVE-2026-5872 — Use-after-free vulnerability in Blink rendering engine
- CVE-2026-3922 — Use-after-free vulnerability in MediaStream
- CVE-2026-5290 — Use-after-free vulnerability in Compositing
- CVE-2026-7363 — Use-after-free vulnerability in Canvas
- CVE-2026-5276 — Insufficient policy enforcement in WebUSB

Fixed Versions

- LTS-144 version 144.0.7559.250 (Platform Version: 16503.82.0)

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/2026/05/long-term-support-channel-update-for.html