مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Security Updates – Chrome OS

Tracking #:432318221

Date:08-01-2026

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 to address multiple security vulnerabilities of **medium to high severity**. The update includes fixes for memory safety issues and implementation flaws that could potentially be exploited by attackers.

Vulnerability Details

- **CVE-2025-38349 (High):** Use-after-free vulnerability with an attack surface on the epoll system call interface.
- **CVE-2025-12443 (Medium):** Out-of-bounds read vulnerability in WebXR.
- **CVE-2025-13720 (Medium):** Bad cast issue in the Loader component.
- **CVE-2025-13632 (Medium):** Inappropriate implementation in DevTools.

Impact

Successful exploitation of these vulnerabilities could lead to memory corruption, application crashes, or potentially arbitrary code execution under certain conditions.

Fixed Version

- LTS version 138.0.7204.300 (Platform Version: 16295.85.0)

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/2026/01/long-term-support-channel-update-for.html