



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Security Updates – Chrome OS

Tracking #:432319067

Date:04-06-2026

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 Chrome OS.

TECHNICAL DETAILS:

Google has released a new Long Term Support (LTS) update for ChromeOS addressing multiple high and critical severity vulnerabilities. The update includes fixes for memory corruption, input validation flaws, race conditions, and sandbox escape risks across core system components such as GPU, networking, extensions, and system services.

Vulnerability Details

Critical Severity

- CVE-2026-9887 – Use after free in Proxy
- CVE-2026-9873 – Use after free in Network
- CVE-2026-9891 – Use after free in Extensions

High Severity

- CVE-2026-9934 – Use after free in Aura
- CVE-2026-9895 – Out of bounds read in GPU
- CVE-2026-9980 – Insufficient validation of untrusted input in Printing
- CVE-2026-10004 – Insufficient validation of untrusted input in Passwords
- CVE-2026-10013 – Use after free in WebCodecs
- CVE-2026-9894 – Use after free in GPU
- CVE-2026-9992 – Use after free in Network
- CVE-2026-9902 – Use after free in Accessibility
- CVE-2026-2314 – Heap buffer overflow in Codecs
- CVE-2026-7351 – Race condition in MHTML
- CVE-2026-10001 – Use after free in Performance Manager

Medium Severity

- CVE-2026-4462 – Out of bounds read in Blink

Successful exploitation of these vulnerabilities could allow an attacker to:

- Execute arbitrary code in ChromeOS processes
- Escalate privileges or bypass sandbox protections
- Intercept or manipulate network traffic
- Access sensitive user data or credentials
- Cause system instability or crashes

Fixed Versions

- LTS-144 version 144.0.7559.254(Platform Version: 16503.86.0)

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/2026/06/long-term-support-channel-update-for.html>