

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Security Updates- Google Chrome

Tracking #:432319316

Date:21-07-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Google has released a Stable Channel security update for the Chrome web browser addressing seven security vulnerabilities, including three Critical and four High severity flaws.

TECHNICAL DETAILS:

Google has released a Stable Channel security update for the Chrome web browser addressing seven security vulnerabilities, including three Critical and four High severity flaws. Several of these vulnerabilities are use-after-free memory corruption issues affecting key Chrome components such as CameraCapture, GPU, Network, Cast, Ozone, Aura, and the V8 JavaScript engine.

Successful exploitation of these vulnerabilities could allow attackers to trigger memory corruption, execute arbitrary code, cause browser crashes, or compromise system security. Users and organizations are strongly advised to update Google Chrome to the latest Stable Channel version immediately to reduce the risk of exploitation.

Vulnerability Details:

- CVE-2026-15899 – Use-After-Free in CameraCapture – Critical
- CVE-2026-15900 – Use-After-Free in GPU – Critical
- CVE-2026-15901 – Use-After-Free in Network – Critical
- CVE-2026-15902 – Use-After-Free in Cast – High
- CVE-2026-15903 – Out-of-Bounds Read and Write in V8 – High
- CVE-2026-15904 – Use-After-Free in Ozone – High
- CVE-2026-15905 – Use-After-Free in Aura – High

Fixed Versions:

- Windows: 150.0.7871.128/.129
- macOS: 150.0.7871.128/.129
- Linux: 150.0.7871.128

RECOMMENDATIONS:

Immediate Actions:

- Update Google Chrome to fixed version or later.

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/>