مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates-Google Chrome

Tracking #:432318913

Date:07-05-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Google has released new Chrome Stable Channel for Windows, Mac, and Linux, addressing 127 security vulnerabilities.

TECHNICAL DETAILS:

Google has released Chrome Stable Channel version 148.0.7778.96/97 for Windows, Mac, and Linux, addressing 127 security vulnerabilities, including multiple Critical and High severity flaws affecting core browser components such as Blink, V8, ANGLE, GPU, DOM, WebRTC, ServiceWorker, and Chromoting.

Vulnerability Details:

- **CVE-2026-7896** — Critical — Integer overflow vulnerability in Blink allowing memory corruption.
- **CVE-2026-7897** — Critical — Use-after-free vulnerability in Mobile component potentially enabling code execution.
- **CVE-2026-7898** — Critical — Use-after-free vulnerability in Chromoting component.
- **CVE-2026-7899** — High — Out-of-bounds read/write vulnerability in V8 JavaScript engine.
- **CVE-2026-7900** — High — Heap buffer overflow vulnerability in ANGLE graphics layer.
- **CVE-2026-7901** — High — Use-after-free vulnerability in ANGLE component.
- **CVE-2026-7902** — High — Out-of-bounds memory access vulnerability in V8.
- **CVE-2026-7903** — High — Integer overflow vulnerability in ANGLE.
- **CVE-2026-7904** — High — Out-of-bounds read vulnerability in Fonts component.
- **CVE-2026-7905** — High — Insufficient validation of untrusted input in Media component.
- **CVE-2026-7906** — High — Use-after-free vulnerability in SVG handling.
- **CVE-2026-7907** — High — Use-after-free vulnerability in DOM component.
- **CVE-2026-7908** — High — Use-after-free vulnerability in Fullscreen component.
- **CVE-2026-7909** — High — Inappropriate implementation issue in ServiceWorker.
- **CVE-2026-7910** — High — Use-after-free vulnerability in Views component.
- **CVE-2026-7911** — High — Use-after-free vulnerability in Aura framework.
- **CVE-2026-7912** — High — Integer overflow vulnerability in GPU component.
- **CVE-2026-7913** — High — Insufficient policy enforcement vulnerability in DevTools.
- **CVE-2026-7914** — High — Type confusion vulnerability in Accessibility component.
- **CVE-2026-7915** — High — Insufficient data validation vulnerability in DevTools.
- **CVE-2026-7916** — High — Insufficient data validation vulnerability in InterestGroups.
- **CVE-2026-7917** — High — Use-after-free vulnerability in Fullscreen component.
- **CVE-2026-7918** — High — Use-after-free vulnerability in GPU component.
- **CVE-2026-7919** — High — Use-after-free vulnerability in Aura framework.
- **CVE-2026-7920** — High — Use-after-free vulnerability in Skia graphics library.
- **CVE-2026-7921** — High — Use-after-free vulnerability in Passwords component.
- **CVE-2026-7922** — High — Use-after-free vulnerability in ServiceWorker.
- **CVE-2026-7923** — High — Out-of-bounds write vulnerability in Skia.
- **CVE-2026-7924** — High — Uninitialized use vulnerability in Dawn graphics subsystem.
- **CVE-2026-7925** — High — Use-after-free vulnerability in Chromoting.
- **CVE-2026-7926** — High — Use-after-free vulnerability in PresentationAPI.
- **CVE-2026-7927** — High — Type confusion vulnerability in Runtime component.

- **CVE-2026-7928** — High — Use-after-free vulnerability in WebRTC.
- **CVE-2026-7929** — High — Use-after-free vulnerability in MediaRecording component.

Fixed Versions:

- Chrome 148.0.7778.96 (Linux)
- 148.0.7778.96/97 Windows/Mac

RECOMMENDATIONS:

Immediate Actions:

- Update all systems to the latest Chrome 148 stable release immediately.
- Enable automatic browser updates across enterprise environments.

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/