مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates-Google Chrome

Tracking #:432319120

Date:12-06-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Google has released new Chrome Stable Channel for Windows, Mac, and Linux, addressing 28 security vulnerabilities across multiple browser components.

TECHNICAL DETAILS:

Google has released Chrome version 149.0.7827.114/.115 for Windows and macOS and version 149.0.7827.114 for Linux, addressing 28 security vulnerabilities across multiple browser components.
The update resolves five Critical and twenty-three High severity vulnerabilities affecting core browser functionality, including Core, GPU, Network, Accessibility, WebMIDI, Media, Extensions, Safe Browsing, Video Processing, Password Management, and DevTools.

Vulnerability Details:

- CVE-2026-12007 — Critical — Use-After-Free in Core
- CVE-2026-12008 — Critical — Use-After-Free in DigitalCredentials
- CVE-2026-12009 — Critical — Insufficient Validation of Untrusted Input in Accessibility
- CVE-2026-12010 — Critical — Heap Buffer Overflow in GPU
- CVE-2026-12011 — Critical — Use-After-Free in WebMIDI
- CVE-2026-12012 — High — Use-After-Free in Network
- CVE-2026-12013 — High — Use-After-Free in Media
- CVE-2026-12014 — High — Use-After-Free in Cast
- CVE-2026-12015 — High — Use-After-Free in Autofill
- CVE-2026-12016 — High — Insufficient Validation of Untrusted Input in DevTools
- CVE-2026-12017 — High — Insufficient Validation of Untrusted Input in Extensions
- CVE-2026-12018 — High — Inappropriate Implementation in Mojo
- CVE-2026-12019 — High — Out-of-Bounds Write in Codecs
- CVE-2026-12020 — High — Use-After-Free in Autofill
- CVE-2026-12022 — High — Race Condition in Safe Browsing
- CVE-2026-12023 — High — Use-After-Free in GPU
- CVE-2026-12024 — High — Insufficient Policy Enforcement in DevTools
- CVE-2026-12025 — High — Insufficient Validation of Untrusted Input in Network
- CVE-2026-12026 — High — Out-of-Bounds Read in Video
- CVE-2026-12027 — High — Insufficient Policy Enforcement in Headless
- CVE-2026-12028 — High — Use-After-Free in GPU
- CVE-2026-12029 — High — Use-After-Free in Video
- CVE-2026-12030 — High — Heap Buffer Overflow in GPU
- CVE-2026-12031 — High — Inappropriate Implementation in Views
- CVE-2026-12032 — High — Inappropriate Implementation in Passwords
- CVE-2026-12033 — High — Out-of-Bounds Read in VideoCapture
- CVE-2026-12034 — High — Insufficient Validation of Untrusted Input in Linux Toolkit Theming
- CVE-2026-12035 — High — Use-After-Free in Views

Fixed Versions:

- Windows/macOS: 149.0.7827.114/.115
- Linux: 149.0.7827.114

RECOMMENDATIONS:

Immediate Actions:

- Update Google Chrome to the latest stable version 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/2026/06/stable-channel-update-for-desktop_01962725236.html