مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates-Google Chrome

Tracking #:432319275

Date:09-07-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Google has released security updates for Windows, macOS, and Linux, addressing 27 security vulnerabilities.

TECHNICAL DETAILS:

Google has released Chrome Stable Channel version 150.0.7871.114/.115 for Windows and macOS, and 150.0.7871.114 for Linux, addressing 27 security vulnerabilities. The update includes two Critical and twenty-three High-severity vulnerabilities, along with two Medium-severity issues.

The most severe vulnerabilities are CVE-2026-15112 and CVE-2026-15129, both Use-After-Free (UAF) flaws affecting the Ozone and Views components. Successful exploitation could result in memory corruption, browser crashes, or potentially arbitrary code execution.

Vulnerability Details:

- CVE-2026-15112 – Critical – Use-After-Free in Ozone
- CVE-2026-15129 – Critical – Use-After-Free in Views
- CVE-2026-15132 – High – Uninitialized Use in V8
- CVE-2026-15133 – High – Use-After-Free in InterestGroups
- CVE-2026-15108 – High – Integer Overflow in Extensions API
- CVE-2026-15109 – High – Uninitialized Use in ANGLE
- CVE-2026-15110 – High – Use-After-Free in Extensions
- CVE-2026-15111 – High – Use-After-Free in Views
- CVE-2026-15113 – High – Use-After-Free in Autofill
- CVE-2026-15114 – High – Out-of-Bounds Read/Write in Codecs
- CVE-2026-15115 – High – Insufficient Validation of Untrusted Input in WebAppInstalls
- CVE-2026-15116 – High – Use-After-Free in Actor
- CVE-2026-15117 – High – Use-After-Free in Payments
- CVE-2026-15118 – High – Use-After-Free in Input
- CVE-2026-15119 – High – Inappropriate Implementation in GetUserMedia
- CVE-2026-15120 – High – Use-After-Free in Core
- CVE-2026-15121 – High – Use-After-Free in WebRTC
- CVE-2026-15122 – High – Insufficient Validation of Untrusted Input in Codecs
- CVE-2026-15123 – High – Insufficient Data Validation in DOM
- CVE-2026-15124 – High – Insufficient Policy Enforcement in Passwords
- CVE-2026-15125 – High – Inappropriate Implementation in Forms
- CVE-2026-15126 – High – Use-After-Free in Forms
- CVE-2026-15127 – High – Inappropriate Implementation in WebGL
- CVE-2026-15128 – High – Inappropriate Implementation in Forms
- CVE-2026-15130 – High – Insufficient Policy Enforcement in Navigation
- CVE-2026-15107 – Medium – Use-After-Free in IndexedDB
- CVE-2026-15131 – Medium – Insufficient Data Validation in Navigation

Fixed Version:

- 150.0.7871.114/.115 for Windows and Mac and 150.0.7871.114 for Linux

RECOMMENDATIONS:

Immediate Actions:

- Update Google Chrome immediately to the latest release.

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/2026/07/stable-channel-update-for-desktop_01162222768.html