مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates-Google Chrome

Tracking #:432319045

Date:01-06-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Google has released new Chrome Stable Channel for Windows, Mac, and Linux, addressing 51 Security Fixes Including 22 Critical Vulnerabilities.

TECHNICAL DETAILS:

Google has released a Stable Channel security update for Chrome addressing 151 security vulnerabilities, including 22 Critical-severity flaws affecting multiple browser components such as GPU, Network, WebGL, ANGLE, Dawn, Bluetooth, Browser, Extensions, WebView, XR, Proxy, Skia, and Base.

Critical Vulnerability Details:

- CVE-2026-9872 — Critical — Out-of-bounds write in GPU leading to memory corruption and potential code execution
- CVE-2026-9873 — Critical — Use-after-free in Network component allowing memory corruption and possible RCE
- CVE-2026-9874 — Critical — Use-after-free in Dawn enabling memory corruption and potential code execution
- CVE-2026-9875 — Critical — Out-of-bounds read in WebGL leading to information disclosure and memory leakage
- CVE-2026-9876 — Critical — Use-after-free in WebGL causing memory corruption and possible crash or code execution
- CVE-2026-9877 — Critical — Use-after-free in ANGLE enabling memory corruption and potential exploitation
- CVE-2026-9878 — Critical — Use-after-free in ANGLE leading to memory corruption and browser instability
- CVE-2026-9879 — Critical — Out-of-bounds write in ANGLE allowing arbitrary memory overwrite
- CVE-2026-9880 — Critical — Insufficient validation of untrusted input in WebGL leading to potential exploitation
- CVE-2026-9881 — Critical — Use-after-free in Bluetooth enabling memory corruption and possible privilege escalation
- CVE-2026-9882 — Critical — Integer overflow in ANGLE leading to memory corruption
- CVE-2026-9883 — Critical — Use-after-free in Base component causing memory corruption and potential RCE
- CVE-2026-9884 — Critical — Use-after-free in Browser component enabling process compromise
- CVE-2026-9885 — Critical — Insufficient input validation in UI allowing security bypass and manipulation
- CVE-2026-9886 — Critical — Use-after-free in Base leading to memory corruption and potential code execution
- CVE-2026-9887 — Critical — Use-after-free in Proxy component enabling browser compromise
- CVE-2026-9888 — Critical — Use-after-free in WebView leading to embedded browser compromise
- CVE-2026-9889 — Critical — Out-of-bounds read/write in Dawn enabling memory corruption and information disclosure

- CVE-2026-9890 — Critical — Use-after-free in XR component leading to memory corruption
- CVE-2026-9891 — Critical — Use-after-free in Extensions allowing sandbox escape and code execution
- CVE-2026-9892 — Critical — Inappropriate implementation in Skia leading to rendering and security issues
- CVE-2026-9893 — Critical — Use-after-free in Skia causing memory corruption and potential RCE

Fixed Versions:

- 148.0.7778.216/217 Windows
- 148.0.7778.215/216 Mac
- 148.0.7778.215 Linux

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/2026/05/stable-channel-update-for-desktop_0877304591.html