مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Actively Exploited Vulnerability in Google Chrome
Tracking #:432317431
Date:01-07-2025

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Google issued a critical security update to address an actively exploited zero-day vulnerability in Google Chrome.

TECHNICAL DETAILS:

Google issued a critical security update to address an actively exploited zero-day vulnerability—CVE-2025-6554—in the V8 JavaScript engine used by Google Chrome. This type confusion vulnerability can enable remote code execution (RCE) if exploited successfully. Google has confirmed that in-the-wild exploitation of this flaw is already underway.

Given the nature of the bug and its exploitation potential, users across Windows, macOS, and Linux are urged to update their browsers immediately to prevent possible compromise via malicious websites or drive-by downloads

Vulnerability Details
- **CVE Identifier:** CVE-2025-6554
- **Severity Level:** High
- **Exploitation Status:** Confirmed to be actively exploited in the wild
- **Vulnerability Type:** Type Confusion
- **Affected Component:** V8 JavaScript Engine (used in Google Chrome)
- **Impact:** May allow **Remote Code Execution (RCE)**
- **Attack Vector:** Malicious web pages, drive-by downloads, sandbox escape techniques
- **Platforms Affected:** Windows, macOS, Linux
- **Patched Chrome Versions:**
    - **Windows:** 138.0.7204.96 / 138.0.7204.97
    - **macOS:** 138.0.7204.92 / 138.0.7204.93
    - **Linux:** 138.0.7204.96

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to update Google Chrome to the latest version.

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/2025/06/stable-channel-update-for-desktop_30.html