مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Zero Day Vulnerability in Google Chrome

Tracking #:432315891

Date:27-05-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Google released emergency security updates to address a new zero-day vulnerability in Google Chrome. This vulnerability is actively exploited in the wild.

TECHNICAL DETAILS:

Google released emergency security updates to address a new zero-day vulnerability (CVE-2024-5274) that is being actively exploited by threat actors. This is the eighth zero-day patched by Google this year.

- **Vulnerability**: **CVE-2024-5274** (type confusion in V8)
- **Severity**: High (critical)
- **Exploited in the wild**: Yes
- **Affected Products**: Chrome Browser (all versions prior to 125.0.6422.112/.113)
- **Patch Available**: Yes (Chrome version 125.0.6422.112/.113 for Windows and macOS, version 125.0.6422.112 for Linux)

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating 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/2024/05/stable-channel-update-for-desktop_23.html