مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Actively Exploited Zero-Day Vulnerability in Google Chrome

Tracking #:432317344

Date:03-06-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Google released a critical security update for the Chrome browser, addressing multiple vulnerabilities, including a high-severity zero-day vulnerability (CVE-2025-5419) that is currently being actively exploited in the wild.

TECHNICAL DETAILS:

Google released a critical security update for the Chrome browser, addressing multiple vulnerabilities, including a high-severity zero-day vulnerability (CVE-2025-5419) that is currently being actively exploited in the wild. The flaw resides in Chrome's V8 JavaScript engine and allows for out-of-bounds read and write operations, potentially leading to arbitrary code execution or sandbox escape.

Google confirmed that an exploit for this vulnerability exists and is being used in targeted attacks, possibly by state-sponsored threat actors. A second, medium-severity vulnerability (CVE-2025-5068) in Chrome's Blink rendering engine was also addressed.

1. **CVE-2025-5419 (Zero-Day - High Severity)**
   - **Type:** Out-of-Bounds Read/Write
   - **Component:** V8 (Chrome's JavaScript engine)
   - **Impact:** Arbitrary code execution, sandbox escape
   - **Exploitation Status: Actively Exploited**

This vulnerability allows attackers to access and manipulate memory outside of the intended buffer boundaries, making it possible to execute malicious code or escape the browser sandbox. The flaw is particularly dangerous when combined with other exploit chains targeting privilege escalation or remote code execution.

2. **CVE-2025-5068 (Medium Severity)**
   - **Type:** Use-After-Free
   - **Component:** Blink (Chrome's rendering engine)
   - **Impact:** Heap corruption, potential remote code execution

Use-after-free vulnerabilities arise when a program continues to use memory after it has been freed. Attackers can exploit this to corrupt memory or execute arbitrary code depending on the context.

Fixed Version: The Stable channel has been updated to 137.0.7151.68/.69 for Windows, Mac and 137.0.7151.68 for Linux

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.html