مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Actively Exploited Zero-Day Vulnerability in Google Chrome

Tracking #:432318124

Date:11-12-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Google has issued an emergency security update for Chrome Desktop to address a zero-day vulnerability that is currently being actively exploited in the wild.

TECHNICAL DETAILS:

Google has released an urgent security update for Chrome Desktop addressing three security vulnerabilities, including a high-severity zero-day (issue 466192044) actively exploited in the wild. The update also includes patches for two medium-severity CVEs affecting the Password Manager and Toolbar components. Immediate deployment of the latest Chrome update is strongly recommended to prevent exploitation.

Zero day Vulnerability Information

1. High-Severity Zero-Day Vulnerability (Issue 466192044)
   - Status: Under coordination (CVE pending)
   - Severity: High
   - Exploitation: Confirmed in the wild
   - Description: Google has not released technical details but confirmed that threat actors are actively exploiting this flaw

Other Vulnerabilities:

2. CVE-2025-14372: - Medium Use after free in Password Manager.
3. CVE-2025-14373: - Medium Inappropriate implementation in Toolbar.

Fixed Versions:

- Stable Channel Update for Desktop
  143.0.7499.109/.110 for Windows/Mac and 143.0.7499.109 for Linux

RECOMMENDATIONS:

- Organizations should treat this advisory with high priority, ensure immediate patch deployment, and enhance monitoring for potential exploitation artifacts.

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/2025/12/stable-channel-update-for-desktop_10.html