مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Critical Vulnerabilities in Google Chrome

Tracking #:432318795

Date:16-04-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Google has released a Stable Channel update for Chrome addressing 31 security vulnerabilities, including multiple critical memory corruption flaws.

TECHNICAL DETAILS:

Google has released a Stable Channel update for Chrome addressing 31 security vulnerabilities, including multiple critical memory corruption flaws. These vulnerabilities such as heap buffer overflows and use-after-free conditions, pose a high risk of remote code execution (RCE) and potential full system compromise.

Vulnerability Summary (Key Entries)

Critical Severity

- **CVE-2026-6296** – Heap buffer overflow in ANGLE (CVSS: Critical)
- **CVE-2026-6297** – Use-after-free in Proxy (CVSS: Critical)
- **CVE-2026-6298** – Heap buffer overflow in Skia (CVSS: Critical)
- **CVE-2026-6299** – Use-after-free in Prerender (CVSS: Critical)
- **CVE-2026-6358** – Use-after-free in XR (CVSS: Critical)

High Severity

- **CVE-2026-6359** – Use-after-free in Video (CVSS: High)
- **CVE-2026-6300** – Use-after-free in CSS (CVSS: High)
- **CVE-2026-6301** – Type confusion in Turbofan (CVSS: High)
- **CVE-2026-6302** – Use-after-free in Video (CVSS: High)
- **CVE-2026-6303** – Use-after-free in Codecs (CVSS: High)
- **CVE-2026-6304** – Use-after-free in Graphite (CVSS: High)
- **CVE-2026-6305** – Heap buffer overflow in PDFium (CVSS: High)
- **CVE-2026-6306** – Heap buffer overflow in PDFium (CVSS: High)
- **CVE-2026-6307** – Type confusion in Turbofan (CVSS: High)
- **CVE-2026-6308** – Out-of-bounds read in Media (CVSS: High)
- **CVE-2026-6309** – Use-after-free in Viz (CVSS: High)
- **CVE-2026-6360** – Use-after-free in FileSystem (CVSS: High)
- **CVE-2026-6310** – Use-after-free in Dawn (CVSS: High)
- **CVE-2026-6311** – Uninitialized use in Accessibility (CVSS: High)
- **CVE-2026-6312** – Insufficient policy enforcement in Passwords (CVSS: High)
- **CVE-2026-6313** – Insufficient policy enforcement in CORS (CVSS: High)
- **CVE-2026-6314** – Out-of-bounds write in GPU (CVSS: High)
- **CVE-2026-6315** – Use-after-free in Permissions (CVSS: High)
- **CVE-2026-6316** – Use-after-free in Forms (CVSS: High)
- **CVE-2026-6361** – Heap buffer overflow in PDFium (CVSS: High)
- **CVE-2026-6362** – Use-after-free in Codecs (CVSS: High)
- **CVE-2026-6317** – Use-after-free in Cast (CVSS: High)

Medium Severity

- **CVE-2026-6363** – Type confusion in V8 (CVSS: Medium)
- **CVE-2026-6318** – Use-after-free in Codecs (CVSS: Medium)
- **CVE-2026-6319** – Use-after-free in Payments (CVSS: Medium)
- **CVE-2026-6364** – Out-of-bounds read in Skia (CVSS: Medium)

Fixed Versions:

- 147.0.7727.101/102 for Windows/Mac and 147.0.7727.101 for Linux

RECOMMENDATIONS:

- Apply Updates Immediately:
  - Upgrade Chrome to fixed version or latest version immediately.

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/