Severity: High

Advisory Type: Security

Chrome WebView Policy Bypass Vulnerability

Advisory Report

TLP: WHITE

SECURITY THREAT ADVISORY COUNCIL (STAC)

Empowering organizations with cutting-edge cybersecurity strategies to combat emerging digital threats effectively.

EXECUTIVE SUMMARY

Google has patched a high-severity Chrome WebView vulnerability that could allow attackers to bypass security policies and compromise applications embedding web content. Immediate patch validation and enterprise-wide deployment should be prioritized to reduce exposure.

- CVE: CVE-2026-0628
- Active Region: Global
- Affected Sector: Technology / Enterprise IT / Application Development
- Affected Product: Google Chrome (WebView <webview> component used in Chrome Apps and embedded web applications)
- Severity: High
- Published Date: January 07, 2026

TECHNICAL DETAILS

- **Target:** Applications, browser-based tools, and enterprise workflows that embed the Chrome WebView (<webview> tag), including Chrome Apps and internally developed applications relying on embedded web content.

- **Root Cause:** A flaw in policy enforcement logic within the Chrome WebView component that fails to consistently apply security restrictions, creating conditions where isolation and sandbox controls can be bypassed.

- **Prerequisite For Exploitation:** An attacker must be able to load or influence malicious web content inside a vulnerable WebView instance, typically through a compromised application, malicious extension, or untrusted embedded URL, and the target system must be running an unpatched Chrome version.

IMPACT

- Bypass of enforced security policies
- Unauthorized access to sensitive data
- Execution of malicious code within applications
- Potential escape from sandboxed environments
- Privilege escalation within affected applications
- Compromise of application integrity and trust boundaries

RECOMMENDATIONS

- Immediately update Google Chrome to the latest stable version across all systems
- Restrict and review applications using WebView for untrusted content
- Apply least-privilege principles to browser and application execution
- Maintain continuous vulnerability monitoring and timely security updates
- Conduct periodical security testing of applications embedding WebView components

REFERENCE

- https://teamwin.in/chrome-webview-vulnerability-allows-hackers-to-bypass-security-restrictions/

SECURE, SCALE, SUCCEED WITH

CONFIDENCE

EnCyb

www.encyb.com/contact-us/ EnCyb soc@encyb.com

www.encyb.com