



TLP: CLEAR

CALIFORNIA CYBERSECURITY INTEGRATION CENTER



CYBER ADVISORY

Thursday September 10, 2026

CAL-CSIC-202609-A-003

Multiple Critical Vulnerabilities Impacting Google Chrome

Remote Code Execution

Zero-Day Vulnerability

Actively Exploited

Patch Available

The California Cybersecurity Integration Center (Cal-CSIC) have identified multiple vulnerabilities affecting Google Chrome in its latest stable channel update ([Chrome 153](#)).¹ A primary concern is CVE-2026-87491, an out-of-bounds write memory corruption flaw discovered in Chromium's V8 JavaScript and WebAssembly engine.² This zero-day vulnerability potentially affects downstream Chromium-based browsers, including Microsoft Edge and Opera.³ Additionally, it carries an CVSS v3.1 base score of 8.8 (High) and has been added to the CISA Known Exploited Vulnerabilities (KEV) catalog due to active exploitation in the wild. Third-party threat analysis exists; however, no verified public Proof-of-Concept (PoC) has been released. Successful exploitation allows a remote attacker to achieve arbitrary code execution within the browser sandbox via a specially crafted HTML webpage.

The Cal-CSIC recommends the following:

1. Verify Updates: Ensure Google Chrome is updated to at least version 153.0.8010[.]36 (Linux) or 153.0.801[.]36/.37 (Windows/macOS).⁴
2. Restart Browser: Have user fully close and restart Chrome to load the latest patch.⁵
3. Downstream Chromium Software: Monitor and apply corresponding baseline updates for Microsoft Edge, Brave, and Opera as vendor builds become available.

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

TLP: CLEAR

Affected Components and Versions

Affected Product	Affected Software	Versions Impacted
Google	Chrome	153.0.8010.36 or Below

Cal-CSIC services are provided at no cost to assist organizations in strengthening their cybersecurity defenses. If you need assistance or wish to verify this communication, please contact us at (833) REPORT-1, or (916) 636-2997. Visit our website for more details: [California Cybersecurity Integration Center | California Governor's Office of Emergency Services](#)

References:

¹ Google; "Chrome Release"; https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html; accessed 10 September 2026

² CVE; "CVE-2026-87491"; <https://www.cve.org/CVERecord?id=CVE-2026-87491>; accessed 10 September 2026

³ CISA; "Known Exploited Vulnerabilities Catalog"; https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-87491; 10 September 2026

⁴ Google; "Stable Channel Update for Desktop"; https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html; accessed 10 September 2026

⁵ Chrome Enterprise; "RelaunchNotification"; <https://chromeenterprise.google/policies/relaunch-notification/>; accessed 10 September 2026

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

TLP: CLEAR