

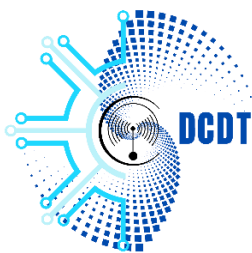
**GOVERNMENT OF THE REPUBLIC
OF VANUATU**

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS
& DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380



**GOUVERNEMENT DE LA
REPUBLIQUE DU VANUATU**

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE
COMMUNICATION ET DE
TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu

Tel: (678) 33380

7 September 2026

**Advisory 261: Google Chrome V8 Type Confusion Zero-Day, Actively Exploited
(CVE-2026-85046).**

Release Date: 4th September 2026

Impact: **CRITICAL**

TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations, System/Network administrators, and all general users of Google Chrome or Chromium-based browsers (including Microsoft Edge, Brave, and Opera, which regularly incorporate the same V8 engine fixes). This alert is intended to be understood by both technical users and systems administrators, and by general staff who simply browse the web.

What is it?

CVE-2026-85046 is a type confusion vulnerability in V8, the JavaScript and WebAssembly engine at the core of Google Chrome, which Google has confirmed is being actively exploited in the wild. The flaw allows a remote attacker to execute arbitrary code inside Chrome's sandboxed renderer process simply by getting a victim to visit a specially crafted HTML page - no download, login, or file execution is required. CERTVU notes those companion fixes for completeness, but these advisory addresses CVE-2026-85046 specifically, since it is the one confirmed to be under active exploitation.

What are the systems affected?

The following version(s) are affected:

- Google Chrome before 152.0.7977.82 (Linux) / 152.0.7977.82 or .83 (Windows and macOS) - (Affected)

Google Chrome 152.0.7977.82/.83 and later - (Not affected, patched)

Chrome normally updates itself automatically in the background, but the update only takes effect after the browser is fully restarted. Given this vulnerability is under active exploitation, do not assume the update has already applied - confirm the installed version directly (<chrome://settings/help>) and prompt a restart on every device where it has not.

What does this mean?

Typical attack flow:

1. **Lure a victim to a malicious or compromised webpage**
 - An attacker delivers a link to a specially crafted HTML page to the victim — for example via a phishing email, a malicious advertisement, or a compromised legitimate website — and the victim opens it in an affected version of Chrome or a Chromium-based browser.
2. **Trigger the V8 type confusion to execute code inside the browser sandbox**
 - JavaScript on the malicious page triggers the type confusion bug in V8 — causing an array to be treated as the wrong internal type — giving the attacker arbitrary read/write access to the JavaScript heap and the ability to execute attacker-controlled code inside Chrome's sandboxed renderer process, without any further action from the victim.

Attack vectors:

- A web-based attack requiring only that the victim visit a malicious or compromised webpage in an affected browser — no file download, credential entry, or software installation is needed.
- Google has confirmed an exploit for this vulnerability exists and is being used in the wild, though it has not disclosed which threat actors or campaigns are involved. Because this code execution occurs inside Chrome's sandbox, a full system compromise would typically require this bug to be chained with a separate sandbox-escape vulnerability — but the browser-level compromise itself is sufficient to expose session data, browsing activity, and anything the victim does inside the browser at the time.

Successful exploitation may allow attackers to:

- Execute arbitrary code inside the Chrome sandbox on the victim's device simply by getting them to view a malicious webpage, with no further interaction required.
- Access data and session activity within the compromised browser process, and potentially pursue a further sandbox-escape exploit chain to gain broader access to the underlying device, depending on the attacker's capability and objectives.

Mitigation process

CERTVU recommends the following:

1. Apply the vendor patch immediately, given confirmed active exploitation
 - Update Google Chrome to version 152.0.7977.82/.83 (Windows/macOS) or 152.0.7977.82 (Linux) or later, via `chrome://settings/help`, and fully restart the browser to complete the update. Given active exploitation, treat this as an emergency update rather than routine patching.
2. Treat this as urgent: CISA has added this CVE to its Known Exploited Vulnerabilities catalog with an 18 September 2026 remediation deadline for US federal agencies — a useful benchmark for any organization's own urgency
3. Update every Chromium-based browser, not just Chrome itself
4. Audit the estate for devices still running an outdated Chrome version
5. Review activity for signs of compromise on any device that may have been exposed

Report suspected compromise to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. <https://www.cve.org/CVERecord?id=CVE-2026-85046>
2. https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_01882797386.html