

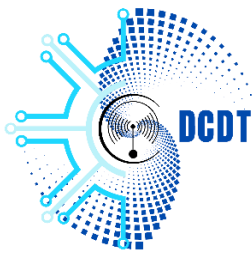
**GOVERNMENT OF THE REPUBLIC
OF VANUATU**

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

10 September 2026

Advisory 286: Google Chrome V8 Out-of-Bounds Write Zero-Day — Actively Exploited (CVE-2026-87491).

Release Date: 9th 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 all users of Google Chrome, including Organizations, System/Network administrators, and members of the general public who browse the web on a Windows, macOS, or Linux device. This alert is intended to be understood by both technical and general readers, and requires urgent action given confirmed active exploitation.

What is it?

CVE-2026-87491 is an out-of-bounds write vulnerability in V8, the JavaScript and WebAssembly engine at the core of Google Chrome and every Chromium-based browser, allowing a remote attacker to execute arbitrary code inside Chrome's sandbox simply by getting a victim to open a specially crafted HTML page. This is the seventh actively-exploited Chrome zero-day patched in 2026.

What are the systems affected?

The following version(s) are affected:

- Google Chrome prior to 153.0.8010.36 (Windows, Linux) - (Affected)
- Google Chrome prior to 153.0.8010.37 (macOS) - (Affected)

Google Chrome 153.0.8010.36/.37 (Windows/macOS) and 153.0.8010.36 (Linux) and later - (Not affected, patched)

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 out-of-bounds write to execute code inside the browser sandbox**
 - JavaScript on the malicious page triggers the out-of-bounds write bug in V8, giving the attacker the ability to corrupt memory and 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 exploited in the wild

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 153.0.8010.36/.37 (Windows/macOS) or 153.0.8010.36 (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. Update every Chromium-based browser, not just Chrome itself
3. Audit the estate for devices still running an outdated Chrome version
4. Review activity for signs of compromise on any device that may have been exposed

Report any suspected compromise arising from this vulnerability to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. <https://www.cve.org/CVERecord?id=CVE-2026-87491>
2. https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html