

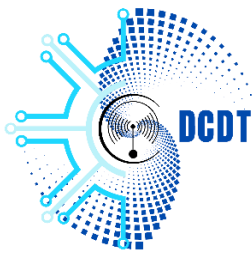
**GOVERNMENT OF THE REPUBLIC
OF VANUATU**

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

9 September 2026

Advisory 277: Google Chrome for Android WebGL Use-After-Free Remote Code Execution (CVE-2026-84352).

Release Date: 2nd 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 for Android, including Organizations, System/Network administrators, and members of the general public who browse the web on an Android device. This alert is intended to be understood by both technical and general readers.

What is it?

CVE-2026-84352 is a critical use-after-free vulnerability in the WebGL component of Google Chrome for Android, allowing a remote attacker to execute arbitrary code outside Chrome's sandbox simply by getting a victim to open a specially crafted HTML page.

CERTVU independently confirmed via Google's own Chrome Releases blog that the fix is available in Chrome 152.0.7977.75 and later for Android.

What are the systems affected?

The following version(s) are affected:

- Google Chrome for Android prior to 152.0.7977.75 - (Affected)

Google Chrome for Android 152.0.7977.75 and later - (Not affected, patched)

What does this mean?

Typical attack flow:

1. **Lure a victim to a crafted web page**
 - An attacker hosts or injects malicious JavaScript/WebGL content on a compromised or attacker-controlled website, and delivers a link to the victim via phishing, malvertising, or a compromised legitimate site.
2. **Trigger the use-after-free and escape the sandbox**
 - Once the victim opens the page in an unpatched Chrome for Android build, the crafted WebGL calls trigger the use-after-free condition, allowing the attacker's code to execute outside the browser's sandbox on the device.

Attack vectors:

- A web-based attack requiring only that the victim visit a malicious or compromised web page in Chrome for Android - via a phishing link, malicious advertisement, or a legitimate site that has itself been compromised.
- No privileges are required and no special access conditions apply beyond the victim opening the page (CVSS AV:N/PR:N/UI:R).

Successful exploitation may allow attackers to:

- Execute arbitrary code outside Chrome's sandbox on the victim's Android device, potentially gaining a foothold to install further malware, access other app data, or exfiltrate photos, credentials, and messages stored on the device.
- Use a compromised personal or work Android device as a pivot point into any government or organizational network the device subsequently connects to (e.g. VPN, work email, or Wi-Fi).

Mitigation process

CERTVU recommends the following:

1. Update Chrome for Android without delay
 - Update Google Chrome for Android to version 152.0.7977.75 or later via the Google Play Store, and confirm the installed version directly rather than assuming it has already updated.
2. Apply the same update guidance to desktop Chrome installations
3. Enable automatic updates on all agency and personal Android devices used for government business
4. Exercise general browsing caution while updates roll out
5. Report suspected compromise

Report any suspected compromise of an Android device used for government business, or any unusual device behaviour following a suspicious web link, to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. <https://www.cve.org/CVERecord?id=CVE-2026-84352>
2. <https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop.html>