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

2 September 2026

Advisory 225: Google Chrome Multiple Critical Vulnerabilities (CVE-2026-79282 and 9 others — see Reference).

Release Date: 25th August 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 Organizations and individual users running Google Chrome on Windows, Mac, or Linux, including government offices and members of the public. This alert is intended to be understood by technical users and systems administrators, though the recommended action is straightforward for any user.

What is it?

Google's Chrome 152 stable channel release fixes 327 security issues in total, ten of which are rated Critical: CVE-2026-79282, CVE-2026-79290, CVE-2026-79054, CVE-2026-79121, CVE-2026-79224, CVE-2026-79052, CVE-2026-79150, CVE-2026-78935, CVE-2026-79012, CVE-2026-79200. Most are use-after-free memory-safety flaws in components including ANGLE (graphics rendering), Aura (window/UI compositing), Chromecast, Views (the UI framework), and Safebrowsing, alongside one critical use-of-uninitialized-variable bug in the Mobile component.

These are memory-corruption bugs that, if triggered by malicious or compromised web content, can potentially be leveraged by an attacker to execute arbitrary code within the browser. The release also addresses roughly 60 further High-severity issues and over 200 Medium- and Low-severity issues; because Chrome ships all fixes in a single build, the same update resolves all of them regardless of severity tier.

What are the systems affected?

The following version(s) are affected:

- Google Chrome prior to 152.0.7977.64 (Linux) – (Affected)
- Google Chrome prior to 152.0.7977.64/.65 (Windows and Mac) – (Affected)

Google Chrome 152.0.7977.64/.65 and later – (Not affected, patched)

Chrome usually updates itself automatically in the background, but the fix only takes effect after the browser is restarted. Users and administrators should not assume they are protected until they have confirmed the version and restarted the browser.

What does this mean?

Typical attack flow:

1. **Trigger the memory-safety flaw**
    - A user visits a malicious or compromised website, or interacts with a malicious Chromecast device or session, causing Chrome to reach a use-after-free or uninitialized-variable condition in one of the affected components.
2. **Exploit the resulting memory corruption**
    - The attacker leverages the corrupted memory state to execute arbitrary code within the browser process, with the potential to chain further bugs to escape Chrome's sandbox depending on the specific component involved.

Attack vectors:

- Visiting a malicious or compromised website - no special user action beyond normal browsing is required for most of these flaws.
- Interacting with a malicious Chromecast device or casting session, for the Chromecast-specific flaws.

Successful exploitation may allow attackers to:

- Execute arbitrary code within the browser process, or crash the browser (denial of service).
- Potentially compromise the host further if a browser exploit is chained with a separate sandbox-escape vulnerability.

Mitigation process

CERTVU recommends the following:

1. Update Chrome and restart the browser

- Confirm Chrome has updated to 152.0.7977.64 or later (152.0.7977.65 on Windows/Mac) via chrome://settings/help, then fully restart the browser so the update takes effect.

2. Push the update fleet-wide in managed environments
3. Enable automatic updates
4. Audit the estate for outdated browsers
5. Monitor Google's Chrome Releases blog for further updates

Reference

1. https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0256176589.html
2. https://www.cve.org/CVERecord?id=CVE-2026-79282
3. https://www.cve.org/CVERecord?id=CVE-2026-79290
4. https://www.cve.org/CVERecord?id=CVE-2026-79054
5. https://www.cve.org/CVERecord?id=CVE-2026-79121
6. https://www.cve.org/CVERecord?id=CVE-2026-79224
7. https://www.cve.org/CVERecord?id=CVE-2026-79052
8. https://www.cve.org/CVERecord?id=CVE-2026-79150
9. https://www.cve.org/CVERecord?id=CVE-2026-78935
10. https://www.cve.org/CVERecord?id=CVE-2026-79012
11. https://www.cve.org/CVERecord?id=CVE-2026-79200