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

3 August 2026

Advisory 177: Google Chrome Multiple Vulnerabilities – Stable Channel Update (Chrome 151, 370 Fixes Including 7 Critical)

Release Date: 29th July 2026
Impact: HIGH
TLP: CLEAR

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

This alert is relevant to Organizations and System/Network administrators that utilize the above products. This alert is intended to be understood by technical users and systems administrators.

What is it?

Google has released Chrome 151 to the Stable channel, fixing 370 security vulnerabilities, including 7 rated Critical, most of which are memory-safety issues (use-after-free, race conditions, and insufficient input validation) in core browser components. This follows Chrome 149 and 150, which together fixed 1,072 flaws, more than the prior 23 milestones combined, a surge Google and researchers attribute in part to AI-assisted vulnerability discovery.

What are the systems affected?

The following product is affected:

- **Google Chrome (Desktop) prior to 151.0.7922.71/.72 (Windows/Mac) or 151.0.7922.71 (Linux)**

The 7 Critical-severity vulnerabilities fixed in this release are:

- CVE-2026-17650: Use after free in Compositing
- CVE-2026-17651: Insufficient validation of untrusted input in Dawn
- CVE-2026-17652: Use after free in Views
- CVE-2026-17653: Use after free in Skia
- CVE-2026-17654: Race condition in Updater
- CVE-2026-17655: Insufficient validation of untrusted input in ANGLE
- CVE-2026-17656: Use after free in Ozone

Chromium-based browsers that share Chrome's rendering engine (e.g. Microsoft Edge, Brave, Opera, Vivaldi) may be affected by the same underlying issues pending each vendor's own release; CERTVU recommends monitoring those vendors' advisories separately.

What does this mean?

Typical exploitation flow for this class of memory-safety vulnerability:

1. Malicious or compromised web content
    - An attacker crafts, or compromises, a webpage or advertisement designed to trigger a memory-corruption condition in a vulnerable Chrome component such as Compositing, Views, Skia, ANGLE, Dawn, or Ozone.
2. Memory corruption triggered
    - Simply visiting the page can trigger the use-after-free, race condition, or input-validation flaw, potentially corrupting process memory.
3. Potential code execution
    - Depending on the specific flaw, successful exploitation could allow arbitrary code execution within the renderer or GPU process, and may need to be chained with a separate sandbox-escape vulnerability for full system compromise.
4. No confirmed in-the-wild exploitation to date
    - Google has not flagged any of the 370 vulnerabilities fixed in this release as actively exploited; however, Critical-severity use-after-free classes are historically prioritised by attackers once patch diffs become public ("n-day" reversal risk), so timely patching remains important.

This vulnerability class typically requires:

- User interaction (visiting a malicious or compromised webpage)
- No prior authentication or account access
- Conditions vary by individual CVE (e.g. some require WebGL/GPU-specific content to reach the ANGLE or Dawn code paths)

Mitigation process

CERTVU recommends the following:

1. **Update Immediately**
    - Ensure all Chrome installations are updated to 151.0.7922.71/.72 (Windows/Mac) or 151.0.7922.71 (Linux) or later. Chrome updates automatically by default; users and administrators should verify the installed version via chrome://settings/help and restart the browser to apply the update.

2. **Enforce Auto-Update Policies**
    - Organizations managing Chrome via enterprise policy (e.g. Google Admin Console, Group Policy) should confirm auto-update channels are not disabled and push the update across the organization without delay.
3. **Monitor Chromium-based Browsers**
    - Track vendor advisories for other Chromium-based browsers in use (Microsoft Edge, Brave, Opera, Vivaldi), as these typically ship equivalent fixes shortly after Google's release.
4. **Practice General Browser Hygiene**
    - Encourage staff to restart their browsers promptly when prompted for updates, and avoid deferring restarts for extended periods, given the volume of memory-safety fixes in this release.

Reference

1. https://chromereleases.googleblog.com/2026/07/stable-channel-update-for-desktop_0887107924.html
2. https://thehackernews.com/2026/07/three-recent-chrome-releases-fix-1442.html
3. https://nvd.nist.gov/vuln/detail/CVE-2026-17650
4. https://www.cisa.gov/known-exploited-vulnerabilities-catalog