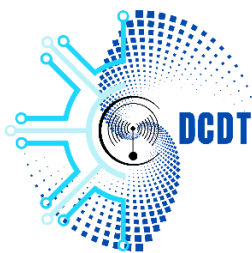


GOVERNMENT OF THE REPUBLIC
OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS
& DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu
Tel: (678) 33380



GOVERNEMENT 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 April 2026

Advisory 126: Google Dawn Use-After-Free Vulnerability

Release Date: 1st April 2026
Impact: **HIGH / 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 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?

CVE-2026-5281 is a high-severity use-after-free vulnerability (CVSS 8.8) affecting the Google Chrome browser. The flaw exists in Dawn, the implementation of the WebGPU (graphics) API used by Chromium-based browsers.

What are the systems affected?

The Vulnerability impacts:

- **Google Chrome versions prior to 146.0.7680.178**
- All platforms running affected Chrome versions, including:
 - Windows
 - macOS
 - Linux

Since Chromium is widely used, other Chromium-based browsers (e.g., Edge, Brave) may also be impacted until patched.

What does this mean?

Exploitation requires user interaction (e.g., visiting a malicious website) and typically involves chaining with another vulnerability.

Typical attack flow:

1. **Delivery via malicious webpage**
 - The attacker hosts or injects a crafted HTML page designed to trigger the flaw.
2. **User interaction**
 - The victim visits the malicious site (phishing, malicious ads, compromised websites).
3. **Renderer process compromise**
 - The exploit targets the Chrome renderer process and triggers the use-after-free condition.
4. **Memory corruption**
 - Freed memory is reused and manipulated by the attacker.
5. **Arbitrary code execution**
 - The attacker executes malicious code within the browser context.

Successful exploitation of CVE-2026-5281 may allow attackers to:

- Execute arbitrary code within the browser
- Access or steal sensitive user data (cookies, sessions, credentials)
- Install malware via browser exploitation chains
- Crash or destabilize the browser
- Potentially escalate to full system compromise (if combined with other exploits)

The vulnerability has also been reported as a **zero-day**, indicating possible real-world exploitation before patch availability.

Mitigation process

CERTVU recommends the following:

1. Apply Security Updates Immediately (Critical)

- Update Google Chrome to:
 - **Version 146.0.7680.178 or later**
- Ensure all Chromium-based browsers are updated accordingly.

Reference

1. <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
2. <https://www.cve.org/CVERecord?id=CVE-2026-5281>