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

20 January 2026

Advisory 117: Microsoft Windows Information Disclosure Vulnerability

Release Date: 13th January 2026
Impact: HIGH / CRITICAL
TLP: CLEAR

The Department of Communication 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-2026-20805 is a security vulnerability in Microsoft Windows' Desktop Window Manager (DWM) where an attacker with local access can disclose sensitive information (memory data) that should be protected. This is classified as an information disclosure flaw, and it was confirmed to be actively exploited in the wild before a patch was issued.

What are the systems affected?

The vulnerability impacts multiple versions of Microsoft Windows running the Desktop Window Manager, including a wide range of Windows 10, Windows 11, and Windows Server editions prior to the January/February 2026 security updates

What does this mean?

To exploit this flaw:

- The attacker must have local authenticated access (i.e., an account on the machine).
- They can abuse the way DWM handles memory to leak memory addresses and other sensitive data.
- This information can help bypass protections such as Address Space Layout Randomization (ASLR), making it easier to chain additional vulnerabilities for privilege escalation or further compromise.

Mitigation process

CERTVU recommend:

1. Apply Microsoft's security updates from the January/February 2026 Patch Tuesday (install the relevant cumulative updates for your Windows versions).
2. Deploy patches urgently
3. Monitor for suspicious behaviour, such as abnormal DWM or local privilege escalation activity.
4. Follow general best practices such as least-privilege accounts and up-to-date endpoint defences to limit lateral use of leaked information.

Reference

.

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://www.cve.org/CVERecord?id=CVE-2026-20805