**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

24 November 2025

## Advisory 111: Microsoft Windows Race Condition Vulnerability

**Release Date:** 12th of November 2025
**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-2025-62215 –** is a race-condition (improper synchronization vulnerability present in the windows kernel. Specifically, multiple threats or processes access a shared kernel resource without proper synchronization, enabling a local attacker to escalate privileges.

# What are the Systems affected?

Affected:

- Supported edition of windows 10, Windows 11, and Windows server (including recent builds) are affected.
- Systems running kernel versions up to (but excluding) certain patched builds are vulnerable.
- Because this is a kernel-level flaw, any workstation or server where a user can execute code locally (or is already compromised to some degree) is at risk of privilege escalation.

# What does this mean?

How attackers exploit this vulnerability (attack vector)

- Attacker must have some level of local code execution or access to be able to exploit the vulnerability (for example a user account or process). The vulnerability is not fully remote from zero access.
- The attacker triggers the race-condition by executing or orchestrating concurrent operation against the shared kernel resource to cause memory corruption or synchronization failure. This can then lead to escalation privileges.
- Once elevated, the attacker can gain full control of the system, bypass application controls, disable security features, install persistent backdoors, move laterally, or use the compromised host as the stepping stone.

# Mitigation process

CERTVU recommend:

Immediate Patching – Apply the Microsoft November 2025 Patch Tuesday

If patching cannot be immediately deployed:

- Restrict user accounts: ensure minimal local user privileges
- Monitor systems for anomalous local privilege escalation indications
- Restrict or disable mechanisms that allow users to load or execute untrusted code locally – This reduces the attack surface.

# Reference


1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://www.cve.org/CVERecord?id=CVE-2025-62215