

**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

23 April 2026

Advisory 131: Microsoft Windows Link Following Vulnerability (CVE-2025-60710).

Release Date: 13th 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-2025-60710 is a high-severity privilege escalation vulnerability (CVSS 7.8) affecting Microsoft Windows systems. The flaw exists in the Host Process for Windows Tasks, due to improper link resolution before file access.

What are the systems affected?

The following version affected;

- Microsoft Windows 11 (notably versions 24H2 and 25H2)
- Systems running vulnerable builds of the Host Process for Windows Tasks

What does this mean?

This is a local privilege escalation (LPE) vulnerability, meaning attackers need some level of access to the system first.

Typical exploitation flow:

1. **Initial access**
 - The attacker gains low-level access (e.g., via malware, phishing, or another vulnerability).
2. **Crafting malicious link or file reference**
 - The attacker creates a symbolic link or manipulated file path that points to a sensitive system resource.
3. **Triggering the vulnerable process**
 - The Windows Host Process incorrectly follows the malicious link during file operations.
4. **Privilege escalation**
 - The attacker redirects operations to protected files or locations, gaining higher (SYSTEM-level) privileges.

Successful exploitation of this vulnerability may allow attackers to:

- Elevate privileges to SYSTEM or administrator level
- Execute arbitrary code with elevated permissions
- Access or modify sensitive system files
- Disable security controls or defenses
- Establish persistence and move laterally within a network

Because it enables privilege escalation, this vulnerability is often used as part of multi-stage attacks following initial compromise.

Mitigation process

CERTVU recommends the following:

1. Apply Microsoft Security Updates (Critical)

- Install the latest Windows security updates addressing CVE-2025-60710 immediately.
- Ensure systems are updated beyond vulnerable builds (e.g., patched versions after 2025 releases).

2. Limit Local Access and Privileges

- Enforce least privilege access for users and applications
- Restrict administrative rights and monitor privilege escalation attempts

Reference

1. <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
2. <https://www.cve.org/CVERecord?id=CVE-2025-60710>
3. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-60710>