

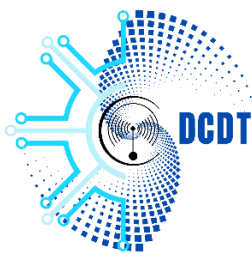
**GOVERNMENT OF THE REPUBLIC
OF VANUATU**

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

9 September 2026

Advisory 275: Windows Advanced Local Procedure Call (ALPC) Heap Buffer Overflow Local Privilege Escalation - Actively Exploited Zero-Day (CVE-2026-85880).

Release Date: 8th September 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, System/Network administrators, and general users of Windows 10, Windows 11, or Windows Server. This alert is intended to be understood by both technical users and systems administrators.

What is it?

CVE-2026-85880 is a high-severity, actively-exploited local privilege escalation vulnerability in Windows Advanced Local Procedure Call (ALPC), a core Windows inter-process communication subsystem, affecting a broad range of Windows versions including Windows 11 (23H2, 24H2, 25H2, 26H1), Windows 10 (versions 1607, 1809, 21H2, and 22H2), and Windows Server (2012, 2012 R2, 2016, 2019, and 2022). The flaw is a heap-based buffer overflow that an attacker who already has low-privileged local access to a system can exploit to escalate their privileges to SYSTEM.

What are the systems affected?

The following version(s) are affected:

- Windows 11 versions 23H2, 24H2, 25H2, and 26H1 (see Microsoft's Security Update Guide for exact affected build ranges) - (Affected)
- Windows 10 versions 1607, 1809, 21H2, and 22H2 (see Microsoft's Security Update Guide for exact affected build ranges) - (Affected)
- Windows Server 2012, 2012 R2, 2016, 2019, and 2022 (see Microsoft's Security Update Guide for exact affected build ranges) - (Affected)

Apply the September 2026 Windows security update, which provides a fixed build for every affected version - (Not affected, patched)

What does this mean?

Typical attack flow:

1. **Obtain initial low-privileged local access to a Windows system**
 - This is a prerequisite for the vulnerability: the attacker must already have some form of local access or code execution on the target, for example via phishing, a separate vulnerability, or a compromised low-privileged account.
2. **Trigger a heap-based buffer overflow in Windows ALPC to escalate to SYSTEM**
 - The attacker sends specially-crafted input to the ALPC subsystem that overflows a heap buffer, corrupting memory in a way that allows the attacker's code to execute with SYSTEM-level privileges.

Attack vectors:

- Local access is required (CVSS AV:L) - this is not a remotely-exploitable flaw on its own, but is significant as a "second stage" in a broader attack chain, letting an attacker who has already gained a foothold (via phishing, a separate remote vulnerability, or a compromised account) escalate to full SYSTEM control.
- No user interaction is required and only low privileges are needed to trigger it once local access is achieved (CVSS PR:L/UI:N). This vulnerability was actively exploited in the wild as a zero-day, before a patch was available, and CERTVU is not aware of any vulnerability-specific public indicators of compromise having been published by its discoverers.

Successful exploitation may allow attackers to:

- Gain full SYSTEM-level privileges on an affected Windows 10, Windows 11, or Windows Server system, effectively taking complete control of the device regardless of the privilege level of the account initially compromised.
- Disable security software, install further malware or persistence mechanisms, and access any data on the system - the same consequences already described for the companion vulnerability, CVE-2026-81963, in Advisory 274.

Mitigation process

CERTVU recommends the following:

1. Apply the September 2026 Windows security update without delay. This vulnerability was actively exploited as a zero-day

- Apply the September 2026 cumulative security update to every affected Windows 10, Windows 11, and Windows Server system via Windows Update, WSUS, or your organisation's patch-management platform, and confirm the fixed build number has actually been applied.

2. Also apply the fix for the companion zero-day, CVE-2026-81963 (Advisory 274), patched in the same September 2026 update

3. Pay particular attention to legacy Windows 10 and Windows Server versions still in use

4. Audit for indicators of a broader compromise chain, not just this flaw in isolation

5. Maintain endpoint detection and response (EDR) coverage on all Windows endpoints

Report suspected compromise to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. <https://www.cve.org/CVERecord?id=CVE-2026-85880>
2. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-85880>