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

12 August 2026

Advisory 185: CVE-2026-68820_Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability

Release Date: 11th August 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 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-2026-68820 is an important-severity elevation of privilege vulnerability in the Windows Ancillary Function Driver for WinSock (afd.sys), the kernel-mode driver that underpins the Windows Sockets (WinSock) networking API
A locally authenticated attacker with low privileges can run a specially crafted application to trigger a race condition in how afd.sys handles socket creation when accessed concurrently by multiple threads. Successful exploitation allows the attacker to gain SYSTEM privileges, with no user interaction required. Microsoft has confirmed this vulnerability was exploited in the wild as a zero-day prior to the 11 August 2026 patch

What are the systems affected?

Affected systems include supported Windows client and server versions, since afd.sys is a core component of the Windows kernel-mode networking stack present on essentially all installations.

Windows 10 (supported versions) – (Affected)
Windows 11 (23H2, 24H2, 25H2, 26H1) – (Affected)
Windows Server 2012 / 2012 R2 – (Affected)
Windows Server 2016, 2019, 2022 – (Affected)
Windows Server 2025, including Server Core installations – (Affected)
x86, x64, and ARM64 editions of the above – (Affected)

Any organisation running unpatched Windows endpoints or servers is at risk, given confirmed active exploitation by a nation-state threat actor.

What does this mean?

This flaw arises from a use-after-free race condition in afd.sys, the driver that manages socket creation for all Windows network communication. An attacker who already has low-privileged local access to a system - for example through phishing, a compromised low-privilege account, or another initial-access technique - can use this bug to gain full SYSTEM control.

Step 1 - Initial Access
The attacker obtains low-privileged local access to the target Windows system through one of the following methods:

- Phishing or social engineering leading to malware execution
- A compromised or low-privilege standard user account
- Chaining from another initial-access or lower-privilege vulnerability

Step 2 - Triggering the Race Condition
The attacker runs a specially crafted application that accesses a socket concurrently from multiple threads while it is being created, exploiting improper synchronisation in afd.sys and freeing memory that is still in use.

Step 3 - Kernel Memory Corruption
By winning the race and reusing the freed kernel memory, the attacker corrupts kernel state in a way that grants control over kernel-mode execution, escalating from a low-privileged process to SYSTEM.

Mitigation process

CERTVU recommends the following:

Primary - Apply August 2026 Security Update Immediately

Install the 11 August 2026 Patch Tuesday cumulative update for your Windows version: KB5121003 (Windows 11 24H2/25H2), KB5121000 (Windows 11 26H1), KB5120240 (Windows 11 23H2), or the equivalent Windows 10 and Windows Server August 2026 cumulative updates. Given confirmed active exploitation by a nation-state actor, this should be treated as an emergency patch rather than deferred to a scheduled maintenance window, prioritising endpoints and servers with direct user or internet exposure.

Microsoft Security Update Guide: CVE-2026-68820

Secondary - Monitor and Restrict Local Access

Until patched, apply the principle of least privilege to reduce the pool of accounts able to run arbitrary code locally, and monitor endpoint detection telemetry for anomalous kernel-mode driver activity, unexpected process privilege escalation, or indicators associated with FudModule rootkit deployment.

Reference

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://www.cve.org/CVERecord?id=CVE-2026-68820
3. https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2026-68820

.