

مجلس الأمن السيبراني  
CYBER SECURITY COUNCIL



**Privilege Escalation Vulnerability in Windows Disk Cleanup Tool**

Tracking #:432316922

Date:03-03-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability, tracked as CVE-2025-21420, has been identified in the Windows Disk Cleanup Tool (cleanmgr.exe), allowing attackers to escalate privileges to SYSTEM.

## TECHNICAL DETAILS:

A high-severity vulnerability, tracked as CVE-2025-21420, has been identified in the Windows Disk Cleanup Tool (cleanmgr.exe), allowing attackers to escalate privileges to SYSTEM.

### Vulnerability Details

- **Vulnerability ID:** CVE-2025-21420
- **Severity:** High (CVSS Score: 7.8)
- **Affected Component:** Windows Disk Cleanup Tool (cleanmgr.exe)
- **Attack Vector:** Local privilege escalation (LPE)
- **Proof-of-concept:** Published on GitHub
- **Exploitation:** Requires execution of a malicious DLL via DLL sideloading
- **Patched Version:** February 2025 Patch Tuesday update

## RECOMMENDATIONS:

The UAE Cyber Security Council recommends to Install the February 2025 Microsoft security updates as soon as possible.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

## REFERENCES:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21420>