



.....
Centre de Veille de Détection et de
Réaction aux Attaques Informatiques

BULLETIN DE SECURITE

Titre	Zero-day affectant Microsoft Windows (Patch Tuesday Décembre 2025)
Numéro de Référence	59111012/25
Date de Publication	10 décembre 2025
Risque	Important
Impact	Critique

Systèmes affectés

- Windows Resilient File System (ReFS)
- Windows Storage VSP Driver
- Windows Shell
- Windows Projected File System
- Windows DWM Core Library
- Windows Cloud Files Mini Filter Driver
- Application Information Service
- Windows File Explorer
- Windows Camera Frame Server Monitor
- Microsoft Brokering File System
- DirectX Graphics Kernel
- Windows DirectX
- DirectX Graphics Kernel
- Windows Defender Firewall Service

Identificateurs externes

CVE-2025-62456	CVE-2025-64673	CVE-2025-59516	CVE-2025-59517	CVE-2025-64661
CVE-2025-62461	CVE-2025-62462	CVE-2025-62464	CVE-2025-55233	CVE-2025-62467
CVE-2025-64679	CVE-2025-64680	CVE-2025-62454	CVE-2025-62457	CVE-2025-62221

CVE-2025-62572 CVE-2025-64658 CVE-2025-62565 CVE-2025-62570 CVE-2025-62469
CVE-2025-62569 CVE-2025-62573 CVE-2025-64670 CVE-2025-62463 CVE-2025-62465
CVE-2025-62468

Bilan de la vulnérabilité

Microsoft annonce la correction de plusieurs vulnérabilités affectant les composants susmentionnés de son système d'exploitation Microsoft Windows. Une de ces vulnérabilités identifiée par « CVE-2025-62221 » et affectant Windows Cloud Files Mini Filter Driver est un « Zero-Day » susceptible d'être activement exploité. Ces vulnérabilités peuvent permettre à un attaquant l'élévation de privilèges, l'exécution de code arbitraire, l'accès à des informations confidentielles ou de causer un déni de service.

Solution

Veillez se référer aux bulletins de sécurité de Microsoft pour obtenir les nouvelles mises à jour.

Risque

- Elévation de privilèges
- Exécution de code arbitraire
- Accès à des informations confidentielles
- Déni de service

Référence

Guide de sécurité de Microsoft :

- <https://msrc.microsoft.com/update-guide/releaseNote/2025-Dec>