



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

BULLETIN DE SECURITE

Titre	Vulnérabilités affectant Microsoft Windows ESU (Patch Tuesday Décembre 2025)
Numéro de Référence	59121012/25
Date de Publication	10 Décembre 2025
Risque	Important
Impact	Critique

Systèmes affectés

- Windows Routing and Remote Access Service (RRAS)
- Windows Remote Access Connection Manager
- Windows Installer
- Windows Common Log File System Driver
- Windows Client-Side Caching
- Win32k
- PowerShell
- Microsoft Message Queuing (MSMQ)
- Windows Routing and Remote Access Service (RRAS)
- Windows Hyper-V

Identificateurs externes

CVE-2025-62549 CVE-2025-64678 CVE-2025-62472 CVE-2025-62474 CVE-2025-62571
CVE-2025-62470 CVE-2025-62466 CVE-2025-62458 CVE-2025-54100 CVE-2025-62455
CVE-2025-62473 CVE-2025-62567

Bilan de la vulnérabilité

Microsoft annonce la correction de plusieurs vulnérabilités affectant les composants susmentionnés de son système d'exploitation Windows. Une de ces vulnérabilités identifiée par « CVE-2025-54100 » est un « Zero-Day » affectant PowerShell. L'exploitation de ces vulnérabilités peut

permettre à un attaquant l'élévation de privilèges, l'exécution de code arbitraire à distance, l'accès à des données confidentielles, l'usurpation d'identité ou le déni de service.

Solution

Veuillez 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 données confidentielles
- Contournement de mesures de sécurité

Référence

Guide de sécurité de Microsoft :

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