



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

## BULLETIN DE SECURITE

<b>Titre</b>	Mise à jour de sécurité pour GnuPG et Gpg4win
<b>Numéro de Référence</b>	60523001/26
<b>Date de Publication</b>	30 Janvier 2026
<b>Risque</b>	Important
<b>Impact</b>	Important

### Systèmes affectés

- GnuPG 2.5.16
- GnuPG 2.5.15
- GnuPG 2.5.14
- GnuPG 2.5.13
- Gpg4win 5.0.0
- Gpg4win 5.0.0-beta479
- Gpg4win 5.0.0-beta476
- Gpg4win 5.0.0-beta395

### Identificateurs externes

- CVE-2026-24881

### Bilan de la vulnérabilité

Une vulnérabilité affectant les versions susmentionnées de GnuPG and Gpg4win a été corrigée. L'exploitation de cette vulnérabilité peut permettre à un attaquant d'exécuter du code à distance ou de causer un déni de service.

## Solution

Veillez se référer à l'éditeur afin d'installer la nouvelle mise à jour

## Risque

- Exécution de code à distance
- Dénî de service

## Références

Bulletin de sécurité GNU :

- <https://lists.gnu.org/archive/html/info-gnu/2026-01/msg00006.html#:~:text=Solution%20====,from%20its%20primary%20file%20server>