



## BULLETIN DE SECURITE

<b>Titre</b>	Vulnérabilité critique affectant le plugin «WPLMS» pour WordPress
<b>Numéro de Référence</b>	50661111/24
<b>Date de publication</b>	11 Novembre 2024
<b>Risque</b>	Critique
<b>Impact</b>	Critique

### Systemes affectés

- Plugin «WPLMS» versions antérieures à 4.963

### Identificateurs externes

- CVE-2024-10470

### Bilan de la vulnérabilité

Une vulnérabilité critique affectant le plugin «WPLMS» pour WordPress a été corrigée. L'exploitation de cette vulnérabilité peut permettre à un attaquant non authentifié d'accéder à des informations confidentielles.

### Solution

Veillez mettre à jour votre plugin à une version non vulnérable.

## Risque

- Accès à des données confidentielles

## Références

Bulletin de sécurité de «Wordfence»

- <https://www.wordfence.com/blog/2024/11/28000-wordpress-sites-affected-by-arbitrary-file-read-and-deletion-vulnerability-in-wplms-wordpress-theme/>