



## BULLETIN DE SECURITE

<b>Titre</b>	Vulnérabilités dans le CMS WordPress
<b>Numéro de Référence</b>	47260605/24
<b>Date de Publication</b>	06 Mai 2024
<b>Risque</b>	Important
<b>Impact</b>	Important

### Systemes affectés

- WordPress versions 6.1.x antérieures à 6.1.6
- WordPress versions 6.2.x antérieures à 6.2.5
- WordPress versions 6.3.x antérieures à 6.3.4
- WordPress versions 6.4.x antérieures à 6.4.4
- WordPress versions 6.5.x antérieures à 6.5.2

### Bilan de la vulnérabilité

Plusieurs vulnérabilités ont été corrigées dans le CMS WordPress. L'exploitation de ces vulnérabilités peut permettre à un attaquant d'injecter du code indirect à distance (XSS).

### Solution

Veillez se référer au bulletin de sécurité WordPress afin d'installer les nouvelles mises à jour.

### Risque

- Injection de code indirecte à distance (XSS)

### Référence

Bulletin de sécurité WordPress:

- <https://wordpress.org/news/2024/04/wordpress-6-5-2-maintenance-and-security-release/>