



## BULLETIN DE SÉCURITÉ

<b>Titre</b>	Vulnérabilités critiques affectant le plugin «UserPro» pour WordPress
<b>Numéro de Référence</b>	45002411/23
<b>Date de Publication</b>	24 Novembre 2023
<b>Risque</b>	Critique
<b>Impact</b>	Critique

### Systemes affectés

- UserPro WordPress Plugin version antérieure à 5.1.2

### Identificateurs externes

- CVE-2023-2437 CVE-2023-2446 CVE-2023-2448 CVE-2023-2449 CVE-2023-6009

### Bilan de la vulnérabilité

WordPress annonce la correction de plusieurs vulnérabilités critiques affectant le plugin «UserPro». Ces vulnérabilités sont activement exploitées et elles peuvent permettre à un attaquant distant d'injecter du code SQL, de réussir une élévation de privilèges et de porter atteinte aux informations confidentielles.

### Solution

Veillez se référer au bulletin de sécurité WordPress du 21 novembre 2023 afin d'installer les nouvelles mises à jour.

### Risque

- Atteinte à la confidentialité des données.
- Élévation de privilèges
- Injection de code SQL

### Annexe

Bulletins de sécurité Wordfence du 21 novembre 2023:

- <https://www.wordfence.com/blog/2023/11/several-critical-vulnerabilities-including-privilege-escalation-authentication-bypass-and-more-patched-in-userpro-wordpress-plugin/>