



## BULLETIN DE SECURITE

|                            |  |
|----------------------------|--|
| <b>Titre</b>               | Vulnérabilité critique affectant le plugin «FluentSMTP» pour WordPress |
| <b>Numéro de Référence</b> | 51102511/24  |
| <b>Date de publication</b> | 25 Novembre 2024   |
| <b>Risque</b>              | Critique   |
| <b>Impact</b>              | Critique   |

### Systemes affectés

- Plugin «FluentSMTP» versions antérieures à 2.2.83

### Identificateurs externes

- CVE-2024-9511

### Bilan de la vulnérabilité

Une vulnérabilité critique affectant le plugin « FluentSMTP » pour WordPress a été corrigée. L'exploitation de cette vulnérabilité peut permettre à un attaquant distant non authentifié d'exécuter du code arbitraire ou d'accéder à des informations confidentielles.

### Solution

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

## Risque

- Exécution de code arbitraire à distance
- Accès à des informations confidentielles

## Références

Bulletin de sécurité de «Wordfence»

- <https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/fluent-smtp/fluentsmtp-wp-smtp-plugin-with-amazon-ses-sendgrid-mailgun-postmark-google-and-any-smtp-provider-2282-unauthenticated-php-object-injection>