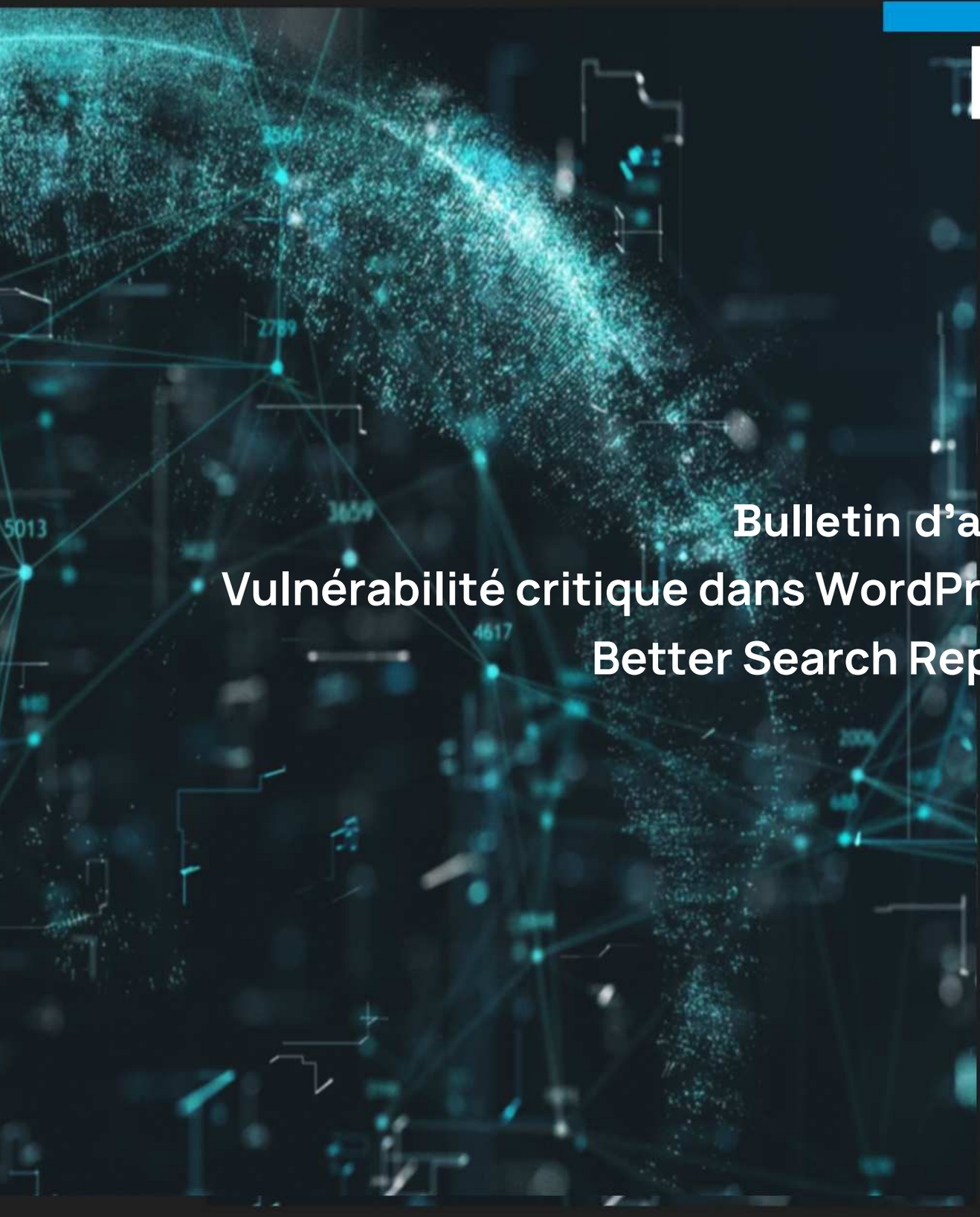
aDvens

Security for the greater good



Bulletin d'alerte

Vulnérabilité critique dans WordPress - Better Search Replace

2024-01-25 | **TLP:CLEAR** | CERT aDvens - CTI
Advens - 16 Quai de la Mégisserie - 75001 Paris

Sommaire

WordPress - Better Search Replace - CVE-2023-6933

Le 24 janvier 2024, Wordfence a publié un bulletin de sécurité concernant la vulnerabilité critique CVE-2023-6933 sur le plugin *Better Search Replace* pour WordPress.

Better Search Replace est installé sur plus d'un million de sites WordPress. Cette extension est utilisée pour faciliter la migration d'une base de données suite à un changement de domaine ou de serveur.

Le chercheur en sécurité Sam Pizzey a identifié une désérialisation non sécurisée dans le plugin, le rendant vulnérable à des injections d'objets PHP.

Il est ainsi possible pour un attaquant non authentifié d'exploiter cette faille. En envoyant des requêtes PHP spécifiquement forgées, ce dernier peut supprimer des fichiers, voler des données sensibles ou exécuter du code arbitraire.

Cette vulnérabilité est activement exploitée.

Wordfence a annoncé avoir bloqué plus de 2551 tentatives d'exploitation de cette vulnérabilité dans les dernières 24 heures.

Type de vulnérabilité

- **CWE-502** : Deserialization of Untrusted Data

Risques

- Exécution de code arbitraire
- Vol de données sensibles
- Suppression de fichiers arbitraires

Criticité (score de base CVSS v3.1)

Vecteur d'attaque	Réseau	Portée	Inchangée
Complexité d'attaque	Faible	Impact sur la confidentialité	Élevé
Privilèges requis	Aucun	Impact sur l'intégrité	Élevé
Interaction de l'utilisateur	Aucune	Impact sur la disponibilité	Élevé

Produits impactés

- Plugin Better Search Replace pour WordPress versions antérieures à 1.4.4 (incluse)

Recommandations

- Mettre à jour le plugin Better Search Replace vers la version 1.4.5 ou ultérieure.
- Des informations complémentaires sont disponibles dans le bulletin de Wordfence.

Preuve de concept

Actuellement, aucune preuve de concept n'est disponible en sources ouvertes.

Références

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-6933
- https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/better-search-replace/better-search-replace-144-unauthenticated-php-object-injection