



BULLETIN D'ALERTE

N° 0426-BA001

Objet	Vulnérabilité critique dans WordPress
Niveau de criticité	CRITIQUE
Référence	CERT-GN-2026-ALT-001
Date de publication	07 avril 2026
Niveau de partage	TLP : WHITE

2. RÉSUMÉ

Le plugin Ninja Forms - File Uploads pour WordPress contient une vulnérabilité dans la fonction '**NF_FU AJAX Controllers Uploads::handle_upload**' en raison de la validation de type de fichier manquant. Cela affecte toutes les versions jusqu'à 3.3.26, ce qui permet aux attaquants non authentifiés de télécharger des fichiers arbitraires sur le serveur affecté.

3. RISQUE DE SÉCURITÉ

Les attaquants non authentifiés peuvent télécharger des fichiers arbitraires sans authentification ni interaction avec l'utilisateur, ce qui peut potentiellement permettre l'exécution de code à distance sur le serveur WordPress affecté. Cela pourrait permettre un compromis complet du site Web et de l'infrastructure du serveur sous-jacent, avec des impacts, y compris le vol de données, la dégradation du site Web, la distribution de logiciels malveillants et le mouvement latéral dans les environnements réseau.

4. CARACTÉRISTIQUES DE LA VULNÉRABILITÉ

Attribut	Valeur
CVE	CVE-2026-0740
Score CVSS v3.1	9.8 (Critique)
Versions affectées	≤ 3.3.26
Version partiellement corrigée	3.3.25
Version entièrement corrigée	3.3.27

5. RECOMMANDATIONS

Mettez immédiatement à niveau le plugin Ninja Forms - File Uploads vers la version 3.3.27 ou version ultérieure. Si le correctif immédiat n'est pas possible, désactivez la fonctionnalité de téléchargement de fichiers jusqu'à ce que le correctif puisse être appliqué. En outre, examinez les journaux du serveur et les fichiers téléchargés pour obtenir des preuves d'exploitation, implémentez des restrictions de téléchargement de fichiers au niveau du serveur Web et surveillez l'exécution de fichiers suspects sur les systèmes affectés.

En cas de difficulté dans l'application des mesures correctives, le GN-CERT se tient à la disposition des entités pour leur apporter l'assistance technique nécessaire.

6. RÉFÉRENCES

- <https://euvd.enisa.europa.eu/enisa/EUVD-2026-19572>
- <https://anssi.gov.gn/bulletin-dinformation/>

