ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité
des Systèmes d'Information

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات

BULLETIN DE SECURITE

Titre	Vulnérabilités dans les plugins WordPress
Numéro de Référence	62502603/26
Date de Publication	26 Mars 2026
Risque	Important
Impact	Important

Systèmes affectés

- Plugin «Masteriyo LMS »versions antérieures à 2.1.7
- Plugin « Nelio A/B Testing » versions antérieures à 8.2.8
- Plugin « PublishPress Revisions » versions antérieures à 3.7.24
- Plugin « Green Downloads » versions antérieures à 2.0.9
- Plugin « JetFormBuilder» versions antérieures à 3.5.6.2
- Plugin « Total Poll Lite » versions antérieures ou égales à 4.12.0
- Plugin « Widget Wrangler » versions antérieures ou égales à 2.3.9
- Plugin « Woody Ad Snippets (Insert PHP » versions antérieures à 2.7.2

Identificateurs externes

- CVE-2026-4484, CVE-2026-32573, CVE-2026-32539, CVE-2026-32536,
- CVE-2026-32525, CVE-2026-27044, CVE-2026-25447, CVE-2026-25366

Bilan de la vulnérabilité

Plusieurs vulnérabilités ont été corrigées dans des plugins et thèmes WordPress. L'exploitation de ces failles peut permettre à un attaquant distant d'exécuter du code arbitraire, contourner l'authentification, voler ou modifier des données sensibles, supprimer du contenu et élever ses privilèges. Ces failles impactent la confidentialité, l'intégrité et la disponibilité des sites WordPress vulnérables.

Solution

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات, مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

Veuillez se référer au bulletin de sécurité WordPress pour plus d'information.

Risque

- Exécution du code arbitraire à distance ;
- Elévation de privilèges ;
- Accès aux informations confidentielles ;
- Compromission de site web ;

Annexe

Bulletins de sécurité WordPress:

- https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/learning-management-system/masteriyo-lms-216-missing-authorization-to-authenticated-student-privilege-escalation-to-administrator
- https://patchstack.com/database/Wordpress/Plugin/nelio-ab-testing/vulnerability/wordpress-nelio-ab-testing-plugin-8-2-7-remote-code-execution-rce-vulnerability?_s_id=cve
- https://patchstack.com/database/Wordpress/Plugin/revisionary/vulnerability/wordpress-publishpress-revisions-plugin-3-7-23-sql-injection-vulnerability?_s_id=cve
- https://patchstack.com/database/Wordpress/Plugin/halfdata-paypal-green-downloads/vulnerability/wordpress-green-downloads-plugin-2-08-arbitrary-file-upload-vulnerability?_s_id=cve
- https://patchstack.com/database/Wordpress/Plugin/jetformbuilder/vulnerability/wordpress-jetformbuilder-plugin-3-5-6-1-remote-code-execution-rce-vulnerability?_s_id=cve
- https://patchstack.com/database/Wordpress/Plugin/totalpoll-lite/vulnerability/wordpress-total-poll-lite-plugin-4-12-0-remote-code-execution-rce-vulnerability?_s_id=cve
- https://patchstack.com/database/Wordpress/Plugin/widget-wrangler/vulnerability/wordpress-widget-wrangler-plugin-2-3-9-remote-code-execution-rce-vulnerability?_s_id=cve
- https://patchstack.com/database/Wordpress/Plugin/insert-php/vulnerability/wordpress-woody-ad-snippets-plugin-2-7-1-remote-code-execution-rce-vulnerability?_s_id=cve