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	62231903/26
Date de Publication	19 Mars 2026
Risque	Important
Impact	Important

Systèmes affectés

- Plugin «Mobile App Editor »versions antérieures ou égales à 1.3.1
- Plugin « BuilderPress » versions antérieures ou égales à 2.0.1
- Plugin « WooCommerce Wholesale Lead Capture » versions antérieures à 2.0.3.2
- Plugin « Woo Blocker Lite / Fraud Prevention for WooCommerce » versions antérieures ou égales à 2.3.2
- Plugin/Thème « Tripgo » versions antérieures à 1.5.6
- Plugin « WP eMember » versions antérieures à 10.2.3
- Plugin « Profile Builder Pro » versions antérieures ou égales à 3.13.9
- Plugin « SlimStat Analytics » versions antérieures à 5.4.0
- Plugin « KiviCare – Clinic & Patient Management System (EHR) » versions antérieures à 4.1.3
- Thème « ColorFolio – Freelance Designer » versions antérieures ou égales à 1.3
- Thème « Traveler » versions antérieures à 3.2.8.1
- Thème « Themeton Finag » versions antérieures ou égales à 1.5.0
- Thème « Themeton Zuut » versions antérieures ou égales à 1.4.2

Identificateurs externes

- CVE-2026-27067, CVE-2026-27065, CVE-2025-60237, CVE-2025-60233, CVE-2026-27542, CVE-2026-27540, CVE-2026-25443, CVE-2026-27093, CVE-2026-28073, CVE-2026-27096, CVE-2026-27413, CVE-2026-1238, CVE-2026-2991, CVE-2026-25449

Bilan de la vulnérabilité

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

Plusieurs vulnérabilités critiques 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

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://patchstack.com/database/wordpress/plugin/mobile-app-editor/vulnerability/wordpress-mobile-app-editor-plugin-1-3-1-arbitrary-file-upload-vulnerability?_s_id=cve
- https://patchstack.com/database/wordpress/plugin/builderpress/vulnerability/wordpress-builderpress-plugin-2-0-1-local-file-inclusion-vulnerability?_s_id=cve
- https://patchstack.com/database/wordpress/theme/finag/vulnerability/wordpress-finag-theme-1-5-0-php-object-injection-vulnerability?_s_id=cve
- https://patchstack.com/database/wordpress/theme/zuut/vulnerability/wordpress-zuut-theme-1-4-2-php-object-injection-vulnerability?_s_id=cve
- https://patchstack.com/database/wordpress/plugin/woocommerce-wholesale-lead-capture/vulnerability/wordpress-woocommerce-wholesale-lead-capture-plugin-1-17-8-privilege-escalation-vulnerability?_s_id=cve
- https://patchstack.com/database/wordpress/plugin/woocommerce-wholesale-lead-capture/vulnerability/wordpress-woocommerce-wholesale-lead-capture-plugin-1-17-8-arbitrary-file-upload-vulnerability?_s_id=cve
- https://patchstack.com/database/wordpress/plugin/woo-blocker-lite-prevent-fake-orders-and-blacklist-fraud-customers/vulnerability/wordpress-fraud-prevention-for-woocommerce-plugin-2-3-2-arbitrary-content-deletion-vulnerability?_s_id=cve
- https://patchstack.com/database/wordpress/theme/tripgo/vulnerability/wordpress-tripgo-theme-1-5-3-local-file-inclusion-vulnerability?_s_id=cve
- https://patchstack.com/database/wordpress/plugin/wp-emember/vulnerability/wordpress-wp-emember-theme-v10-2-2-reflected-cross-site-scripting-xss-vulnerability?_s_id=cve

- https://patchstack.com/database/wordpress/theme/colorfolio/vulnerability/wordpress-colorfolio-freelance-designer-wordpress-theme-theme-1-3-deserialization-of-untrusted-data-vulnerability?_s_id=cve
- https://patchstack.com/database/wordpress/plugin/profile-builder-pro/vulnerability/wordpress-profile-builder-pro-plugin-3-13-9-sql-injection-vulnerability?_s_id=cve
- https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/wp-slimstat/slimstat-analytics-535-unauthenticated-stored-cross-site-scripting-via-fh
- https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/kivicare-clinic-management-system/kivicare-clinic-patient-management-syst em-ehr-412-unauthenticated-authentication-bypass-via-social-login-token
- https://patchstack.com/database/wordpress/theme/traveler/vulnerability/wordpress-traveler-theme-3-2-8-php-object-injection-vulnerability?_s_id=cve