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 critiques dans les plugins WordPress
Numéro de Référence	63790405/26
Date de Publication	04 Mai 2026
Risque	Critique
Impact	Critique

Systèmes affectés

- Plugin « temporary-login » versions antérieures à 1.1.0
- Plugin « wp-editor » versions antérieures à 1.2.9.3
- Plugin «nex-forms-express-wp-form-builder» versions antérieures à 9.1.12
- Plugin « salon-booking-system » versions antérieures à 10.30.26
- Plugin «paid-memberships-pro » versions antérieures à 3.6.6
- Plugin « geo-mashup» versions antérieures à 1.13.20
- Plugin « brizy » versions antérieures à 2.8.12
- Plugin « armember-membership » versions antérieures ou égale 4.0.60
- Plugin « royal-elementor-addons » versions antérieures à 1.7.1058
- Plugin « extended-widget-options » versions antérieures à 5.3.3
- Plugin « widget-options » versions antérieures à 4.2.3
- Plugin « profile-builder-pro » versions antérieures à 3.14.6
- Plugin « pixelYoursite-Pro » versions antérieures à 12.5.0.2
- Plugin « gravityforms » versions antérieures à 2.10.1
- Plugin « import-users-from-csv-with-meta » versions antérieures à 2.0.9
- Plugin « user-verification » versions antérieures à 2.0.47
- Plugin « wp-mail-gateway » versions antérieures à 1.8.1
- Plugin « user-registration-advanced-fields » versions antérieures à 1.6.21

Identificateurs externes

- CVE-2026-7567, CVE-2026-5063, CVE-2026-6320, CVE-2026-4100, CVE-2026-4062, CVE-2026-4061, CVE-2026-4060, CVE-2026-5324, CVE-2026-7649, CVE-2026-6229, CVE-2026-2052, CVE-2026-7647, CVE-2026-7049, CVE-2026-5113, CVE-2026-5112, CVE-2026-5111, CVE-2026-5110, CVE-2026-5109, CVE-2026-7641, CVE-2026-7458, CVE-2026-6963, CVE-2026-4882, CVE-2026-3772

Bilan de la vulnérabilité

Plusieurs vulnérabilités critiques ont été corrigées dans les plugins susmentionnés du CMS 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://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/temporary-login/temporary-login-100-authentication-bypass-to-account-takeover
- https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/nex-forms-express-wp-form-builder/nex-forms-9111-unauthenticated-stored-cross-site-scripting-via-post-parameter-key-
- https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/salon-booking-system/salon-booking-system-free-version-103025-unauthenticated-arbitrary-file-read-via-booking-file-field-path-traversal
- https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/paid-memberships-pro/paid-memberships-pro-365-missing-authorization-to-authenticated-subscriber-stripe-webhook-deletion-and-payment-processing-disruption
- https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/geo-mashup/geo-mashup-11318-unauthenticated-time-based-sql-injection-via-object-ids-parameter

- https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/geo-mashup/geo-mashup-11318-unauthenticated-time-based-sql-injection-via-map-post-type-parameter
- https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/geo-mashup/geo-mashup-11318-unauthenticated-time-based-sql-injection-via-sort-parameter
- https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/brizy/brizy-page-builder-2811-unauthenticated-stored-cross-site-scripting-via-fileupload-field-value
- https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/armember-membership/armember-4060-unauthenticated-sql-injection-via-orderby-parameter
- https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/royal-elementor-addons/royal-addons-for-elementor-171057-authenticated-contributor-server-side-request-forgery-via-csv-url-parameter
- https://www.wordfence.com/threat-intel/vulnerabilities/detail/widget-options-422-authenticated-contributor-remote-code-execution-via-display-logic
- https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/profile-builder-pro/profile-builder-pro-3145-unauthenticated-php-object-injection
- https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/pixelyoursite-pro/pixelyoursite-pro-12501-unauthenticated-blind-server-side-request-forgery-via-urls-
- https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/gravityforms/gravity-forms-2100-unauthenticated-stored-cross-site-scripting-via-consent-field-hidden-input
- https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/gravityforms/gravity-forms-2100-unauthenticated-stored-cross-site-scripting-via-calculation-product-field-in-repeater
- https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/gravityforms/gravity-forms-2100-unauthenticated-stored-cross-site-scripting-via-hidden-product-field-in-repeater
- https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/gravityforms/gravity-forms-2100-unauthenticated-stored-cross-site-scripting-via-single-product-field-inside-repeater
- https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/gravityforms/gravity-forms-2100-unauthenticated-stored-cross-site-scripting-via-product-option
- https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/import-users-from-csv-with-meta/import-and-export-users-and-customers-208-authenticated-subscriber-privilege-escalation-via-multisite-capability-meta-fields
- https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/user-verification/user-verification-by-pickplugins-2046-unauthenticated-authentication-bypass-via-otp-verification-rest-api-endpoint

- https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/wp-mail-gateway/wp-mail-gateway-18-missing-authorization-to-authenticated-subscriber-smtp-configuration-modification-via-wmg-save-provider-config-ajax-action
- https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/user-registration-advanced-fields/user-registration-advanced-fields-1620-unauthenticated-arbitrary-file-upload
- https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/wp-editor/wp-editor-1292-cross-site-request-forgery-to-remote-code-execution-via-plugin-and-theme-file-editor