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	47622705/24
Date de Publication	27 Mai 2024
Risque	Critique
Impact	Critique

Systèmes affectés

- WordPress Copymatic version antérieure à 1.7
- Pie Register version antérieure à 1.7.8
- Hash Form version antérieure à 1.1.1
- Country State City Dropdown CF7 version antérieure à 2.7.3
- WPZOOM Addons for Elementor version antérieure à 1.1.38
- Business Directory version antérieure à 6.4.3
- UserPro version antérieure à 5.1.9
- Fluent Forms Contact Form
- Web Directory Free version antérieure à 1.7.0

Identificateurs externes

- CVE-2024-2771 CVE-2024-31351 CVE-2024-3495 CVE-2024-3552 CVE-2024-35700 CVE-2024-4443 CVE-2024-4544 CVE-2024-5084 CVE-2024-5147

Bilan de la vulnérabilité

Plusieurs vulnérabilités critiques ont été corrigées dans les plugins du CMS WordPress susmentionnés. Un attaquant pourrait exploiter ces failles afin de télécharger des fichiers arbitraires sur un site web, d'extraire des informations sensibles et de porter atteinte à la confidentialité des données ou réussir une élévation de privilèges.

Solution

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

Risque

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

- Prise de contrôle du système affecté
- Exécution du code arbitraire à distance
- Atteinte à la confidentialité des données
- Elévation de privilèges

Annexe

Bulletins de sécurité des plugins WordPress:

- https://patchstack.com/database/vulnerability/copymatic/wordpress-copymatic-plugin-1-6-unauthenticated-arbitrary-file-upload-vulnerability?_s_id=cve
- https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/pie-register-social-site/pie-register-social-sites-login-add-on-177-authentication-bypass
- https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/hash-form/hash-form-drag-drop-form-builder-110-unauthenticated-arbitrary-file-upload-to-remote-code-execution
- https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/country-state-city-auto-dropdown/country-state-city-dropdown-cf7-272-unauthenticated-sql-injection
- https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/wpzoom-elementor-addons/wpzoom-addons-for-elementor-templates-widgets-1137-unauthenticated-local-file-inclusion
- https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/business-directory-plugin/business-directory-plugin-easy-listing-directories-for-wordpress-642-unauthenticated-sql-injection-via-listingfields-parameter
- https://patchstack.com/database/vulnerability/userpro/wordpress-userpro-plugin-5-1-8-unauthenticated-account-takeover-vulnerability
- https://patchstack.com/database/vulnerability/fluentform/wordpress-fluentform-plugin-5-1-16-missing-authorization-to-settings-update-and-limited-privilege-escalation-vulnerability
- https://patchstack.com/database/vulnerability/web-directory-free/wordpress-web-directory-free-plugin-1-7-0-unauthenticated-sql-injection-vulnerability