Autorité Nationale de Cybersécurité

Djibouti le, 23-05-2026

BULLETIN ALERTES

Object	Multiples vulnérabilités dans les plugins WordPress
Réference	1477
Date de Publication	2026-05-22
Sévérité	Critique

IMPACT :

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

SYSTÉME AFFECTÉ :

- Plugin « easy-elements » versions antérieures ou égale 1.4.5 ;
- Plugin « erp-pro » versions antérieures ou égale 1.5.1 ;
- Plugin « bookingpress-appointment-booking-pro » versions antérieures à 5.7 ;
- Plugin « WP Directory Kit » versions antérieures à 1.5.1 ;
- Plugin « divi-form-builder » versions antérieures à 5.1.3 ;

DÉSCRIPTION :

Plusieurs vulnérabilités critiques ont été identifiées dans divers plugins WordPress. Leur exploitation pourrait permettre à un attaquant distant d'obtenir des privilèges administrateur, d'exécuter des injections SQL, de téléverser des fichiers malveillants et de compromettre totalement les sites affectés.

SOLUTION :

Mettre à jour les plugins WordPress (se référer à la documentation).

DOCUMENTATION :

- Bulletins de sécurité WordPress:

https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/easy-elements/easy-elements-for-elementor-addons-website-templates-145-unauthenticated-privilege-escalation-via-custom-meta-parameter

https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/erp-pro/wp-erp-pro-151-unauthenticated-sql-injection-via-search-key-parameter

https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/bookingpress-appointment-booking-pro/bookingpress-pro-56-unauthenticated-arbitrary-file-upload-via-signature-custom-field

https://patchstack.com/database/wordpress/plugin/wpdirectorykit/vulnerability/wordpress-wp-directory-kit-plugin-1-5-0-sql-injection-vulnerability?_s_id=cve

https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/divi-form-builder/divi-form-builder-512-unauthenticated-privilege-escalation-via-role

- CVE-2026-9018:

https://www.tenable.com/cve/CVE-2026-9018

- CVE-2026-4834:

https://www.tenable.com/cve/CVE-2026-4834

- CVE-2026-6960:

https://nvd.nist.gov/vuln/detail/CVE-2026-6960

- CVE-2026-39531:

https://app.opencve.io/cve/CVE-2026-39531

- CVE-2026-5118 :

  https://www.tenable.com/cve/CVE-2026-5118