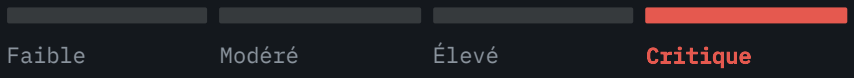
RempartWP

Rapport — audit de sécurité approfondi

equipement-atlantique.example

Site public et serveur, évalués avec un accès temporaire en lecture seule. Aucune modification.



Risque global : Critique

Préparé pour
equipement-atlantique.example

Date
12 octobre 2026

Référence
IWS-20261012-13B6

Classification
Confidentiel. Réservé au propriétaire du site.

Préparé par
RempartWP, sécurité WordPress, Cork, Irlande

Exemple de rapport. Le site est fictif ; les failles et les avis de sécurité cités sont réels et publics.

1 Synthèse

Le site a été compromis, et l'attaquant a toujours accès. Une porte dérobée a été plantée dans le dossier des téléversements en novembre 2025, un compte administrateur a été créé le même jour, et la page de connexion a été modifiée pour enregistrer les mots de passe. Le point d'entrée le plus probable est une vieille extension de gestion de fichiers, désactivée mais jamais supprimée — une extension désactivée reste accessible.

Rien ne suggère que des données de cartes ont été prises : les paiements sont traités sur les pages de Stripe. Mais les noms, adresses et historiques de commande des clients étaient à portée. Agissez aujourd'hui sur les quatre premiers constats, dans l'ordre, et lisez la note sur le RGPD sous F-01.

Constats par gravité

Critique	4	Exploitable dès maintenant, généralement sans se connecter, et mène au contrôle complet du site ou de ses données. À corriger immédiatement.
Élevée	0	Une faiblesse sérieuse qui donne à un attaquant une voie réaliste vers le site ou ses données. À corriger sous quelques jours.
Moyenne	3	Une faiblesse qui aide un attaquant ou demande des conditions particulières pour être exploitée. À corriger dans la semaine.
Faible	1	Durcissement et bonnes pratiques. Aucune voie directe de compromission en soi. À corriger dans le mois.
Conforme	7	Points vérifiés où rien ne demandait d'attention.

Site	https://equipement-atlantique.example/
Date de l'évaluation	12 octobre 2026
Périmètre	Site public et serveur, évalués avec un accès temporaire en lecture seule. Aucune modification.
Méthode	Chaque constat a été vérifié à la main, avec un compte temporaire fourni pour cet audit et supprimé ensuite. Rien n'a été exploité ni modifié sur le site en production.
Risque global	**Critique**

2 Constats détaillés

Les constats sont classés par ordre de priorité. Chacun indique ce qui a été observé, ce que cela signifie pour le site, et comment le corriger.

F-01 Une porte dérobée est cachée dans le dossier des téléversements

Critique

Concerné	`wp-content/uploads/2025/11/wp-cache-helper.php`
Preuve	Un fichier PHP dans un dossier qui ne devrait contenir que des images. Il décode et exécute tout ce qu'on lui envoie (eval de données POST décodées en base64). Date du fichier : 3 novembre 2025.
Impact	Celui qui l'a planté peut exécuter n'importe quel code sur le serveur quand il le souhaite, sans se connecter — lire la base de données, modifier le site ou envoyer du spam depuis celui-ci. Corriger les autres problèmes sans retirer celui-ci laisse la porte ouverte.
Recommandation	Faites une sauvegarde complète à titre de preuve, puis supprimez le fichier et cherchez dans le reste de wp-content d'autres fichiers PHP dans uploads. Changez chaque mot de passe lié au site : administrateurs WordPress, hébergement, base de données, SFTP.
Effort estimé	1 heure, avec les étapes de F-02 et F-03
Note du relecteur	Des données personnelles de clients étaient à portée de l'attaquant. Selon le RGPD, une violation qui présente un risque pour les droits des clients doit être notifiée à l'autorité de contrôle (la CNIL en France, l'APD en Belgique) dans les 72 heures suivant sa découverte — un appel rapide à votre conseil dès aujourd'hui s'impose.

F-02 Un compte administrateur que personne ne reconnaît

Critique

Concerné	`Utilisateur « wp_support2 » (administrateur)`
Preuve	Créé le 3 novembre 2025 à 02 h 14 — la même nuit que la porte dérobée de F-01. Enregistré avec une adresse e-mail jetable ; dernière connexion le 6 octobre 2026.
Impact	L'attaquant dispose d'un chemin d'accès normal, distinct de la porte dérobée, et l'a utilisé récemment.
Recommandation	Supprimez le compte (attribuez son contenu à un utilisateur existant), puis générez de nouvelles clés de sécurité WordPress dans wp-config.php pour déconnecter toutes les sessions, et réinitialisez tous les mots de passe administrateur.
Effort estimé	15 minutes

F-03 2 fichiers du cœur de WordPress ont été modifiés

Critique

Concerné	`wp-login.php, wp-includes/class-wp-hook.php`
Preuve	Les 3 071 fichiers du cœur ont été comparés aux sommes de contrôle de WordPress.org pour la 6.8.3 ; ces deux-là diffèrent. wp-login.php écrit chaque identifiant et mot de passe saisis dans un fichier caché ; class-wp-hook.php charge la porte dérobée de F-01.
Impact	Chaque mot de passe tapé sur la page de connexion depuis la modification a été enregistré. C'est pourquoi réinitialiser les mots de passe avant de nettoyer ces fichiers ne servirait à rien.
Recommandation	Réinstallez le cœur de WordPress (Tableau de bord → Mises à jour → Réinstaller), ce qui remplace les deux fichiers, puis réinitialisez tous les mots de passe — dans cet ordre.
Effort estimé	15 minutes

F-04 L'extension File Manager désactivée est le point d'entrée probable

Critique

Concerné	`Extension WP File Manager 6.0, inactive (actuelle : 8.0.2)`
Preuve	Installée mais désactivée. Son composant vulnérable répond toujours à son adresse par défaut. Les journaux du serveur montrent des requêtes vers lui les 2 et 3 novembre 2025, juste avant l'apparition de la porte dérobée.
Impact	N'importe qui, sans se connecter, peut téléverser des fichiers et exécuter du code via cette extension. Désactiver une extension ne supprime pas ses fichiers : la faille est restée ouverte.
Recommandation	Supprimez entièrement l'extension (Extensions → Supprimer), et faites-en une règle : supprimez les extensions que vous n'utilisez pas plutôt que de les désactiver.
Effort estimé	5 minutes
Avis de sécurité	`9.8` Unauthenticated Arbitrary File Upload leading to Remote Code Execution `(CVE-2020-25213)`, corrigé dans 6.9

F-05 Les fichiers des extensions et du thème sont modifiables depuis le tableau de bord

Moyenne

Concerné	`wp-config.php`
Preuve	DISALLOW_FILE_EDIT n'est pas défini, donc Apparence → Éditeur de fichiers du thème et Extensions → Éditeur de fichiers des extensions sont disponibles pour chaque administrateur.
Impact	Quiconque entre dans un compte administrateur peut modifier le code du site sans toucher au serveur — exactement ce qui rend un mot de passe volé si dangereux.
Recommandation	Ajoutez define('DISALLOW_FILE_EDIT', true); dans wp-config.php.
Effort estimé	5 minutes

F-06 Trop d'administrateurs, aucun avec double authentification

Moyenne

Concerné	`Utilisateurs`
Preuve	5 comptes administrateurs en plus de F-02. Deux ne se sont pas connectés depuis plus d'un an ; un est partagé par l'équipe de la boutique. Aucun n'utilise la double authentification.
Impact	Chaque compte administrateur est une clé complète de la boutique. Les comptes inutilisés et partagés sont ceux dont les mots de passe fuient sans que personne ne s'en aperçoive.
Recommandation	Supprimez les deux comptes inutilisés, donnez à chaque personne son propre accès avec le rôle le plus bas qui convient (Gestionnaire de boutique pour le traitement des commandes), et activez la double authentification pour chaque administrateur.
Effort estimé	30 minutes

F-07 Les e-mails de @equipement-atlantique.example peuvent être falsifiés

Moyenne

Concerné	`DNS de equipement-atlantique.example`
Preuve	SPF : v=spf1 include:_spf.google.com ~all DMARC : v=DMARC1; p=none — mode observation seulement DKIM : trouvé (sélecteur « google »)
Impact	N'importe qui peut envoyer un e-mail qui semble venir de la boutique — confirmations de commande, demandes de remboursement — et les destinataires reçoivent l'instruction de le délivrer quand même. Après une compromission, les clients sont une cible probable d'hameçonnage.
Recommandation	Passez l'enregistrement DMARC à p=quarantine dès maintenant, puis à p=reject une fois que les rapports montrent qu'aucun envoi légitime n'échoue.
Effort estimé	10 minutes

F-08 3 extensions ne sont pas à jour

Faible

Concerné	`WooCommerce 10.1.2 → 10.2.1 ; Mailchimp for WooCommerce 5.4 → 5.5 ; Smash Balloon Instagram Feed 6.9.1 → 6.10`
Preuve	Aucune faille publiée ne touche ces versions aujourd'hui.
Impact	Rien de connu ne touche encore ces versions — les garder à jour est ce qui fait que cela reste vrai.
Recommandation	Mettez-les à jour après le nettoyage, avec une sauvegarde d'abord ; activez les mises à jour mineures automatiques pour WooCommerce.
Effort estimé	15 minutes

3 Points vérifiés sans problème

- ✓ Cœur WordPress 6.8.3 : à jour ; les 3 069 autres fichiers du cœur correspondent à la version officielle
- ✓ Thème actif et son parent : à jour, aucune faille connue, aucun fichier modifié
- ✓ 18 extensions actives : aucune faille connue, aucun fichier différent des copies de WordPress.org
- ✓ Base de données : aucun script injecté ni lien de spam dans les articles, pages, widgets ou options
- ✓ Aucun autre fichier PHP dans uploads ; aucune tâche planifiée inattendue (cron)
- ✓ Paiements : traités sur les pages hébergées par Stripe — les données de cartes ne transitent jamais par le site
- ✓ Sauvegardes quotidiennes hors site par l'hébergeur, 30 derniers jours disponibles

4 Plan de correction

Aujourd'hui	F-01	Une porte dérobée est cachée dans le dossier des téléversements
	F-02	Un compte administrateur que personne ne reconnaît
	F-03	2 fichiers du cœur de WordPress ont été modifiés
	F-04	L'extension File Manager désactivée est le point d'entrée probable
Cette semaine	F-05	Les fichiers des extensions et du thème sont modifiables depuis le tableau de bord
	F-06	Trop d'administrateurs, aucun avec double authentification
	F-07	Les e-mails de @equipement-atlantique.example peuvent être falsifiés
Ce mois-ci	F-08	3 extensions ne sont pas à jour

A Annexe : composants détectés

Les logiciels identifiés sur le site, la version installée et la version actuelle au moment de l'évaluation.

Composant	Type	Installée	Actuelle	Avis
WordPress	Cœur	6.8.3	6.8.3	0
Storefront Child	Thème	1.0	n/d	0
Storefront	Thème	4.6.1	4.6.1	0
WP File Manager (inactive)	Extension	6.0	8.0.2	1
WooCommerce	Extension	10.1.2	10.2.1	0
WooCommerce Stripe Gateway	Extension	9.8.1	9.8.1	0
Mailchimp for WooCommerce	Extension	5.4	5.5	0
Smash Balloon Instagram Feed	Extension	6.9.1	6.10	0
Yoast SEO	Extension	26.1	26.1	0
WP Mail SMTP	Extension	4.6.0	4.6.0	0
Complianz GDPR	Extension	7.4.2	7.4.2	0

B Annexe : périmètre, méthode et limites

Chaque constat a été vérifié à la main, avec un compte temporaire fourni pour cet audit et supprimé ensuite. Rien n'a été exploité ni modifié sur le site en production.

Les journaux de l'hébergeur ne remontent qu'à 30 jours avant l'audit, plus les journaux archivés de novembre 2025 fournis par l'hébergeur ; l'activité entre ces deux périodes n'a pas pu être examinée.

L'inventaire ci-dessus liste les composants liés aux constats ; la liste complète des 21 extensions a été vérifiée.

Les données de failles viennent de WPVulnerability (CC0) et du répertoire d'extensions de WordPress.org. De nouvelles failles sont publiées chaque semaine : ce rapport décrit le site au 12 octobre 2026 seulement.