Matrice de mise à jour, d’exposition et d’audit WordPress

Versions corrigées, signaux de compromission, contrôles et actions prioritaires.

Zone	Situation / version	Risque ou signal	Contrôle recommandé	Commande / emplacement	Action prioritaire
Cœur	7.0 à 7.0.1	Deux CVE combinables ; exposition critique sans authentification.	Lire la version active depuis l’instance, pas depuis une documentation interne.	wp core version	Installer 7.0.2 immédiatement.
Cœur	6.9 à 6.9.4	Primitive SQL et confusion REST présentes.	Confirmer la branche et l’état des mises à jour automatiques.	Tableau de bord > Mises à jour	Installer 6.9.5 immédiatement.
Cœur	6.8 à 6.8.5	Primitive SQL présente ; confusion REST critique absente.	Ne pas conclure que 6.8 est saine : le premier défaut reste corrigé en 6.8.6.	wp core check-update	Installer 6.8.6 immédiatement.
Cœur	< 6.8	Non touché par ces avis précis, mais branche dangereusement obsolète.	Inventorier PHP, thème, extensions et compatibilité avant migration.	wp core version --extra	Planifier une montée de version urgente.
Sauvegarde	Avant toute opération	Une mise à jour ou une réponse à incident sans retour arrière augmente le risque.	Sauvegarder base, wp-content, configuration et journaux hors du serveur.	Outil hébergeur + sauvegarde immuable	Tester la restauration, pas seulement la création.
Intégrité	Fichiers du cœur	Fichier modifié ou ajouté dans wp-admin / wp-includes.	Comparer tous les fichiers aux sommes officielles de la version active.	wp core verify-checksums --include-root	Isoler puis remplacer le cœur depuis une source officielle.
Intégrité	Extensions WordPress.org	Fichier d’extension altéré après compromission.	Comparer les checksums ; interpréter séparément les extensions premium ou privées.	wp plugin verify-checksums --all --strict	Réinstaller proprement toute extension douteuse.
Extensions	Installations récentes	Nouvelle extension, MU-plugin ou plugin désactivé inconnu.	Lister nom, statut, version et date de fichiers ; contrôler wp-content/mu-plugins.	wp plugin list; répertoire wp-content	Désactiver seulement après conservation des preuves.
Thèmes	Thèmes actifs et inactifs	Backdoor dissimulée dans functions.php ou un thème inutilisé.	Lister les thèmes et comparer les fichiers aux sources de confiance.	wp theme list	Supprimer les thèmes inutiles après analyse.
Utilisateurs	Administrateurs	Compte, e-mail ou date d’inscription inconnus.	Exporter tous les comptes administrateurs et leurs métadonnées.	wp user list --role=administrator	Suspendre le compte, préserver les traces, réinitialiser les accès.
Capacités	Rôles détournés	Utilisateur non admin doté de capacités élevées.	Contrôler rôles, usermeta et capacités personnalisées.	wp user list --fields=ID,user_login,roles	Révoquer les capacités anormales et rechercher leur origine.
Tâches	WP-Cron	Hook inconnu, récurrence courte ou argument encodé.	Exporter les événements avec dates, récurrences et arguments.	wp cron event list --fields=hook,next_run,recurrence	Documenter puis supprimer uniquement les hooks malveillants confirmés.
Redirections	Site, accueil, règles	Redirection vers un domaine tiers ou comportement réservé à certains visiteurs.	Comparer siteurl/home ; examiner .htaccess, Nginx, plugins SEO et snippets.	wp option get siteurl; wp option get home	Neutraliser la règle et vérifier cache/CDN.
Contenu	Articles, widgets, options	JavaScript injecté, iframe, option autoload suspecte.	Comparer avec une sauvegarde saine et rechercher les modifications récentes.	wp post list; export base en lecture seule	Conserver une copie forensic avant nettoyage.
REST	Journaux d’accès	Accès anormaux au endpoint batch et paramètres d’auteur.	Filtrer les requêtes REST autour de la date de publication et avant le patch.	Logs proxy / CDN / serveur web	Corréler IP, user-agent, heure, réponse et requêtes suivantes.
Authentification	Sessions actives	Cookie volé ou session persistante après création de compte.	Révoquer les sessions et renouveler les secrets après collecte des preuves.	wp config shuffle-salts	Forcer la reconnexion de tous les utilisateurs.
Identifiants	Admin, SFTP, SSH, base	Un accès persiste hors de WordPress.	Inventorier tous les chemins d’administration et clés déployées.	Panneau hébergeur, IAM, authorized_keys	Rotation coordonnée depuis un poste sain.
Infrastructure	PHP et droits fichiers	Écriture trop large facilitant la persistance ou la RCE.	Contrôler propriétaire, groupe, permissions et fonctions PHP sensibles.	Audit hébergeur / configuration PHP-FPM	Réduire les droits après restauration fonctionnelle.
Mise à jour	Automatique forcée	L’interface peut annoncer une tentative sans prouver le succès.	Vérifier version, e-mail d’update, Site Health et erreurs de fichiers.	Outils > Santé du site; wp core version	Confirmer le résultat sur chaque instance et chaque nœud.
Cache / CDN	Après correctif	Ancienne réponse, origine non patchée ou nœud oublié.	Purger les caches et inventorier toutes les origines / conteneurs.	Console CDN, orchestration, load balancer	Patcher chaque réplique avant remise en trafic.
Preuves	Incident suspecté	Nettoyage prématuré détruisant la chronologie.	Capturer logs, copies de fichiers, horodatages et export base en lecture seule.	Snapshot hébergeur + stockage hors ligne	Préserver la preuve avant toute suppression.
Retour en ligne	Après remédiation	Persistance résiduelle malgré un cœur à jour.	Rejouer les checksums, scanner les comptes, tâches, logs et sorties réseau.	Checklist complète + supervision	Surveiller renforcé pendant plusieurs jours.