BULLETIN DE VEILLE N°12

ANPT-2025-BV-12

"The human factor is the weakest link in cybersecurity.."
— Bruce Schneier

Décembre 2025

Alertes de sécurité

Wordpress

Une vulnérabilité de WordPress expose les sites à des risques de piratage

17 décembre 2025

Une importante faille de sécurité a été signalée dans le thème Motors utilisé sur des milliers de sites WordPress, cette vulnérabilité, trackée sous CVE-2025-64374, affecte les versions jusqu'à 5.6.81 et antérieures, et permet à des utilisateurs disposant de privilèges minimaux (abonnés ou "Subscriber") de contourner les contrôles d'accès et d'installer ou activer des plugins malveillants. La faille réside dans un gestionnaire AJAX qui autorise l'installation de plugins via une fonction backend, mais qui ne vérifie pas correctement les permissions avant d'exécuter l'opération. La validation repose uniquement sur un nonce, qui est censé prévenir les attaques CSRF mais ne remplace pas une vérification de permission adéquate, et ce nonce est accessible à des comptes non privilégiés via l'interface d'administration ; ceci permet à des utilisateurs peu autorisés de fournir une URL de plugin arbitraire pour l'installer et l'activer, ouvrant la porte à un takeover complet du site.

Le thème Motors, développé par StylemixThemes et installé sur plus de 20 000 sites actifs, est donc exposé à ce risque critique tant que les administrateurs n'ont pas appliqué la mise à jour corrective.

L'incident met en lumière des problèmes structurels récurrents dans les thèmes et extensions WordPress, où des mécanismes de sécurité basés uniquement sur des nonces sont indûment utilisés pour valider des actions sensibles sans contrôle de permissions adéquat. Alors que les nonces servent à prévenir la falsification de requêtes, ils ne doivent pas être utilisés comme unique moyen de décision d'accès, souligne la documentation officielle de WordPress. Les administrateurs de sites doivent non seulement appliquer les correctifs publiés, mais aussi revoir régulièrement leurs pratiques de sécurité : limiter les comptes utilisateurs avec privilèges élevés, n'accorder que les permissions nécessaires, auditer les thèmes et plugins installés, et utiliser des solutions de sécurité complémentaires pour détecter et bloquer les comportements suspects.

Source : https://bit.ly/4smapaz

MongoDB

MongoDB recommande aux administrateurs de corriger immédiatement une vulnérabilité grave.

24 décembre 2025

MongoDB a émis une alerte urgente demandant aux administrateurs de mettre immédiatement à jour leurs serveurs en raison d'une vulnérabilité de haute gravité, identifiée comme CVE-2025-14847, qui affecte de nombreuses versions de MongoDB Server et MongoDB. Cette faille provient d'un mauvais traitement des entêtes compressés zlib dans le protocole réseau, ce qui peut amener le serveur à renvoyer des morceaux de mémoire non initialisés lorsque des paquets malformés sont envoyés.

La vulnérabilité est jugée critique car elle peut être exploitable à distance sans authentification et avec une complexité d'attaque faible, ce qui signifie qu'un acteur malveillant n'a pas besoin de droits préalables pour tenter une compromission. Les versions antérieures à MongoDB 8.2.3, 8.0.17, 7.0.28, 6.0.27, 5.0.32 et 4.4.30 sont touchées, et toute instance auto-hébergée exécutant l'une des versions vulnérables avec la compression zlib activée doit être considérée comme à risque élevé.

Pour réduire l'exposition, MongoDB recommande une mise à jour immédiate vers les versions corrigées listées ci-dessus et, comme solution temporaire lorsque la mise à jour n'est pas possible, désactiver la compression zlib, ce qui neutralise le chemin de code vulnérable mais peut affecter les performances réseau. En complément du patching, les administrateurs doivent restreindre l'accès réseau aux instances MongoDB, n'exposer que des clients de confiance, appliquer des contrôles d'accès et des niveaux d'authentification forts, et surveiller les logs pour détecter toute activité suspecte en lien avec des paquets compressés irréguliers.

Source : https://bit.ly/3MS8iLH

Actualité

La violation des données de Shinhan Card en Corée du Sud touche 192 000 commerçants

Un important incident de fuite de données a été confirmé par Shinhan Card, une des principales sociétés de cartes de crédit en Corée du Sud, affectant environ 190 000 à 192 000 commerçants affiliés à ses services. L'entreprise a indiqué qu'elle avait signalé l'incident à la Personal Information Protection Commission après avoir identifié des signes de fuite lors de la vérification d'un rapport d'intérêt public, et qu'elle coopère pleinement avec les autorités dans le cadre de l'enquête. Selon l'analyse interne, l'origine du problème ne serait pas une cyberattaque externe, mais plutôt une mauvaise utilisation interne des données par des employés, qui ont partagé des informations personnelles de commerçants — comme noms, numéros de téléphone mobile, adresses d'entreprise et dates de naissance — pour des activités de démarchage et de recrutement de nouveaux clients entre mars 2022 et mai 2025.

Le rapport de l'entreprise et des régulateurs souligne que ces données ne comprendraient pas d'informations sensibles telles que les numéros de carte bancaire, les numéros d'accès ou les informations financières directes, ce qui signifie qu'à ce stade aucune évidence d'usage frauduleux n'a été confirmée. Shinhan Card a toutefois mis en place des pages en ligne permettant aux commerçants de vérifier s'ils sont concernés par la fuite. L'incident a mis en lumière des lacunes potentielles dans les contrôles internes et la gouvernance des données, car la fuite a perduré pendant plus de trois ans avant d'être détectée, déclenchant des critiques sur la protection de l'information et la surveillance des pratiques des employés impliqués.

La réponse institutionnelle s'est accélérée : la Financial Services Commission et le Financial Supervisory Service ont tenu des réunions d'urgence, lancé une inspection sur site de Shinhan Card, et examinent la possibilité d'actions correctives et de sanctions si des violations de la loi coréenne sur la protection des données sont avérées. Les autorités ont aussi demandé à l'entreprise de renforcer ses mesures pour prévenir tout préjudice secondaire, notamment en alertant les personnes affectées contre le phishing ou d'autres tentatives d'escroquerie utilisant les données exposées. Shinhan Card a retiré les employés impliqués de leurs fonctions et assure qu'elle envisagera des poursuites pénales si nécessaire, tout en s'engageant à améliorer ses procédures de sécurité afin d'éviter que des incidents similaires ne se reproduisent.

Source : https://bit.ly/4sjsgir

Environ 1 000 systèmes compromis lors d'une attaque par ransomware contre l'agence roumaine de l'eau

Un important incident de ransomware a frappé Administrația Națională Apele Române (Romanian Waters), l'autorité nationale en charge de la gestion des ressources hydriques en Roumanie. Les autorités ont confirmé qu'environ 1 000 systèmes informatiques — incluant des serveurs d'applications géographiques, des bases de données, des postes de travail Windows, des serveurs de messagerie et des serveurs web — ont été compromis par des attaquants, entraînant le chiffrement de fichiers et l'affichage de demandes de rançon. L'attaque a débuté le 20 décembre 2025 et s'est propagée rapidement à dix des onze administrations régionales de bassins fluviaux, laissant les équipes informatiques dans une course contre la montre pour isoler les machines touchées et tenter de récupérer les systèmes toujours utilisables. Malgré l'ampleur du compromis, les opérations essentielles de gestion de l'eau — comme le fonctionnement des barrages, l'approvisionnement en eau potable et la surveillance des niveaux d'eau — n'ont pas été interrompues, car elles ont été assurées localement par les équipes sur site hors du réseau central compromis. Les autorités ont souligné que l'absence d'intégration de ces systèmes au cadre national de cybersécurité pour les infrastructures critiques avait exposé inutilement l'administration à ce risque.

L'attaque a été qualifiée de ransomware, même si aucune identification claire du groupe ou de la charge offensive n'a été publiée : des notes de rançon ont été laissées sur les machines chiffrées, exigeant une négociation sous sept jours. Les responsables roumains ont conseillé de ne pas engager de négociations avec les auteurs, car cela pourrait encourager davantage d'extorsions sans garantir la récupération des données. Pendant que l'enquête se poursuit, l'agence nationale de cybersécurité (DNSC) a recommandé des mesures d'urgence telles que la restauration à partir de sauvegardes propres, la vérification intégrale des systèmes pour détecter toute présence persistante, et l'intégration future de ces réseaux dans les systèmes de surveillance nationale afin d'anticiper et bloquer des attaques similaires. L'incident met en lumière la vulnérabilité des infrastructures publiques non protégées par des cadres de défense robustes, et devrait inciter d'autres opérateurs d'infrastructures critiques à renforcer leurs stratégies de cybersécurité, segmentation réseau, surveillance des anomalies et réponse aux incidents.

Source :https://bit.ly/4pewOnp

Bon à savoir

Protégez vos comptes : ne partagez jamais vos codes OTP et méfiez-vous du phishing

Les mots de passe à usage unique (OTP) constituent une couche de sécurité essentielle pour protéger les comptes en ligne contre les accès non autorisés. Les cybercriminels cherchent toutefois à tromper les utilisateurs en leur demandant ces codes via des messages anonymes, SMS frauduleux, e-mails ou appels téléphoniques. Ces messages jouent souvent sur l'urgence, en prétendant qu'un compte est bloqué, qu'une activité suspecte a été détectée ou qu'une action immédiate est requise. En

réalité, aucune entreprise légitime ne demande un OTP par message ou par téléphone. Partager un seul code peut suffire à permettre à un attaquant de se connecter, de changer les identifiants et de voler des informations personnelles ou financières. Il est donc crucial de comprendre qu'un OTP est strictement personnel et confidentiel.

Les attaques de phishing deviennent de plus en plus crédibles, imitant des banques, des réseaux sociaux ou des services officiels. Les fraudeurs utilisent des logos, un ton professionnel et parfois des numéros ou adresses falsifiés pour inspirer confiance. Certains indices doivent alerter : fautes d'orthographe, liens raccourcis, expéditeur inhabituel ou demande d'informations sensibles. Il est fortement déconseillé de cliquer sur des liens ou d'ouvrir des pièces jointes provenant de messages inattendus. La bonne pratique consiste à se connecter directement via le site officiel ou l'application du service concerné afin de vérifier l'information. L'activation des filtres anti-spam et des alertes de connexion renforce également la protection.

Pour se protéger efficacement, il faut refuser systématiquement de partager un OTP, quelle que soit la situation. En cas de message suspect, il est préférable de le supprimer et, si possible, de le signaler au service concerné. L'utilisation d'applications d'authentification plutôt que des codes SMS offre une sécurité accrue contre l'interception. Il est aussi recommandé de vérifier régulièrement les paramètres de sécurité de ses comptes et de sensibiliser son entourage aux techniques d'escroquerie. Adopter une attitude prudente, prendre le temps de réfléchir avant d'agir et se rappeler qu'un service légitime ne demandera jamais un OTP sont des réflexes essentiels pour éviter le phishing et le vol de comptes.

Evènements

Evènement à venir

International Conference on Big Data, IoT, Cyber Security and Information Technology (ICOBDICSIT)

03 Janvier 2026 | Blida, Algeria

https://bit.ly/4jopAMv

La Conférence internationale sur le Big Data, l'IoT, la cybersécurité et les technologies de l'information est une organisation importante qui œuvre à l'avancement du domaine des sciences et des technologies. Elle encourage les étudiants et les jeunes chercheurs à s'engager dans des activités de recherche. Elle offre des ressources pour approfondir les recherches, des financements pour les chercheurs confrontés à des contraintes économiques et un mentorat pour soutenir et guider les projets de recherche. Elle aide également les chercheurs à publier leurs travaux dans des revues et des conférences de grande qualité.

Référence	ANPT-2025-BV-12
Titre	Bulletin de veille N°12
Date de version	31 Décembre 2025
Contact	ssi@anpt.dz