TLP:CLAIR

Urgence de la distribution MOYENNE (partage dans les 24 heures)

25 mars 2026

Avis de cybersécurité – Conseils et pratiques exemplaires pour WordPress

Sommaire

Il a récemment été signalé que certaines organisations qui exploitent des sites Web basés sur WordPress ont subi des incidents de sécurité résultant de mauvaises configurations et de failles connexes. Le présent avis de sécurité contient des conseils et des pratiques exemplaires recommandées afin d'aider à réduire l'exposition aux risques associés et à les atténuer.

Les systèmes de gestion de contenu restent des cibles fréquentes pour les pirates, qui exploitent les composants obsolètes, les failles d'authentification, les erreurs de configuration, le manque de surveillance et une gouvernance insuffisante de la part des fournisseurs. Dans certains cas, du code malveillant peut être introduit pour modifier le comportement du site, par exemple en y affichant des versions différentes de pages ou en diffusant des logiciels malveillants. La mise en œuvre des pratiques exemplaires permet de réduire l'exposition aux risques et de renforcer la cyber-résilience en général.

Comment cela touche-t-il mon organisation?

- Un code malveillant peut être inséré dans un site Web afin d'afficher des versions différentes ou cachées du contenu en fonction de la source de provenance ou du comportement de l'utilisateur.
- Les pirates peuvent tenter des attaques par embuscade en modifiant des sites Web de confiance afin de diffuser des logiciels malveillants par le biais de téléchargements automatiques.

- Un site Web qui expose des ports ou des services inutiles augmente le risque de balayage automatisé et d'exploitation.
- Des thèmes ou des composants obsolètes au cœur de WordPress élargissent considérablement la surface d'attaque.
- Une authentification faible et l'absence d'authentification multifactorielle augmentent considérablement le risque de compromission des identifiants administratifs.
- Une journalisation insuffisante réduit la visibilité sur les modifications non autorisées ou les activités malveillantes.
- Les environnements d'hébergement gérés par des fournisseurs peuvent ne pas appliquer les correctifs ou les mesures appropriées de renforcement ou de surveillance.

Que dois-je faire?

Dès que possible :

- **Transmettez le présent avis** à vos équipes responsables de la cybersécurité, des opérations réseau et des technologies de l'information.
- Demandez-leur **d'examiner, d'évaluer et de mettre en œuvre** des mesures appropriées d'atténuation des risques, notamment :
    - Imposer l'authentification multifactorielle pour tous les accès administratifs.
    - Appliquer les correctifs aux modules d'extension et thèmes du cœur de WordPress et supprimer les composants inutilisés ou non pris en charge.
    - S'assurer que les portails d'administration sont protégés par un VPN ou un pare-feu et ne sont pas directement exposés à Internet.
    - Désactiver les fonctions d'édition de fichiers dans l'interface d'administration WordPress et appliquer des permissions de fichiers strictes.
    - Activer la journalisation détaillée des événements d'authentification, des modifications de fichiers et de configuration, ainsi que de l'activité des plugins.

- Passer en revue tous les systèmes exposés à Internet et fermer les ports ou services inutiles.
- Confirmer les responsabilités des fournisseurs en matière de mise à jour, de surveillance et de réponse aux incidents, et s'assurer que celles-ci sont documentées.
- Conserver des sauvegardes hors ligne sécurisées et testées afin de restaurer des versions propres du site Web si un code malveillant est détecté.

Si vous avez besoin de conseils supplémentaires ou de recommandations propres à un secteur d'activité, nous pouvons vous aider à assurer le suivi.

Détails techniques

Acteurs malveillants et TTP :

- Un code malveillant peut présenter de manière sélective un contenu différent à certains utilisateurs, permettant ainsi aux attaquants de dissimuler leurs activités nuisibles aux administrateurs.
- Les attaques par embuscades peuvent consister à injecter des scripts destinés à diffuser des logiciels malveillants aux visiteurs du site par le biais de téléchargements automatiques.
- Les attaquants recherchent systématiquement les modules d'extension ou les thèmes obsolètes ou vulnérables ou les erreurs de configuration, et ils les exploitent pour obtenir un accès initial.
- Les fichiers malveillants injectés dans les répertoires des sites Web peuvent être utilisés pour maintenir la persistance ou modifier le comportement du site.
- Les identifiants administratifs compromis permettent de modifier les modèles, d'insérer des scripts ou de capturer des données.
- Les sites qui présentent des ports ou des services excessivement exposés offrent aux attaquants davantage d'occasions de reconnaissance et d'exploitation.

Plus d'informations :

- Hardening WordPress (en anglais)
- WordPress Security Hardening 2026: The Complete Guide From Server to Application (en anglais)
- How to improve WordPress security (en anglais)
- Securing WordPress (en anglais)

Action recommandée

Recommandations supplémentaires :

- Activer l'authentification multifactorielle, y compris sur les services de gestion de contenu, lorsque cela est possible.
- Appliquer rapidement les correctifs de sécurité sur l'ensemble des systèmes.
- Les connexions sortantes doivent être limitées aux seules destinations professionnelles autorisées.
- Rédaction d'un plan d'intervention en cas de cyberincident.
- Assurez-vous que vous disposez de sauvegardes fonctionnelles et récentes.
- Veiller à ce que les solutions de protection des postes et les logiciels anti-malware soient à jour.
- Sensibiliser le personnel à la détection des tentatives de hameçonnage et des messages suspects.

Autres renseignements

Le Centre d'excellence en cybersécurité dispose d'un portail, Cybersécurité Ontario, qui offre aux professionnels des TI et de la sécurité de même qu'aux responsables de la gestion du changement dans le secteur parapublic de l'Ontario une formation de base sur la cybersécurité.

Le portail Cyber Sécurité Ontario est administré par le Centre d'excellence en cybersécurité de la Division de la cybersécurité du ministère des Services au public et aux entreprises et de l'Approvisionnement de l'Ontario.

Pour savoir comment le Centre d'excellence en cybersécurité renforce la cybersécurité dans le secteur parapublic, consultez le site Centre d'excellence en cybersécurité.

Aucune garantie

Le présent avis de cybersécurité peut contenir du contenu et des liens provenant de tiers. Le Centre d'excellence en cybersécurité ne contrôle pas et ne maintient pas les liens avec des tiers et ne fait aucune déclaration ni ne donne aucune garantie quant à la validité de ces liens : (a) fonctionnera encore lorsque vous cliquerez dessus; ou (b) fournira un service ou un contenu utile, approprié, exempt de virus ou fiable. Il vous incombe de déterminer si vous souhaitez accéder à un lien ou accepter de recevoir ou de vous fier à un service ou à un contenu mis à votre disposition.

Le Centre d'excellence en cybersécurité fournit de l'information sur une menace connue en vue d'une utilisation potentielle, à la seule discrétion des destinataires, pour se protéger contre les cybermenaces. Cet avis a pour but d'aider les organisations du secteur parapublic à se préparer et à résister à la cybercriminalité.

Définitions

Les menaces ou les incidents de cybersécurité sont des événements qui présentent un risque à la sécurité (p. ex. confidentialité, disponibilité ou intégrité) des ressources d'information, des systèmes et des réseaux d'une organisation.

- L'avis de **menace** à la cybersécurité est communiqué **lorsqu'aucune attaque active** n'est observée. L'avis de menace a pour but de permettre aux organisations de se préparer à faire face à des cybermenaces et de les atténuer.
- L'avis **d'incident** de cybersécurité est communiqué lorsqu'une **attaque active** est observée. Ces renseignements doivent être communiqués rapidement. L'avis d'incident a pour but d'informer les organisations d'un incident de cybersécurité en cours afin que l'organisation puisse se préparer à une intervention et à l'adoption de mesures correctrices en temps opportun.

Le Centre d'excellence en cybersécurité utilise le protocole TLP (Traffic light protocol) pour le partage d'information avec des parties externes au gouvernement de l'Ontario; il désigne l'information sur les programmes publiques par la mention « TLP:CLAIR » et l'information surcon les programmes non publique par la mention « TLP:VERT ».