Type de Contenu	Description
Titre	***Une vulnérabilité de sévérité critique identifiée dans un plugin WordPress expose actuellement plusieurs sites WordPress.***
ID	*202407/AS/06*
Code TLP	*Green*
Niveau de Risque	***Critique***
Application et service affectés	***Plugin WordPress "Email Subscribers by Icegram Express - Email Marketing, Newsletters, Automation for WordPress & WooCommerce"***
Version/Edition	*Versions antérieures à la version 5.7.25 incluse.*
Plateforme	***WordPress & WooCommerce <= 5.7.25***
Mise à jour	*Passer urgemment à la version 5.7.26, ou à une version ultérieure.*
Résumé	*Cette vulnérabilité permet à des attaquants non authentifiés d'exécuter des attaques d'injection SQL programmées, leur permettant d'ajouter des requêtes SQL supplémentaires aux requêtes existantes.*
Impacts	• ***Exécution des attaques d'injection SQL programmées;*** • ***Exfiltration des informations sensibles de la base de données;*** • ***Violation de données importantes, entraînant la fuite d'informations sensibles.***
Description Détaillée	*Une vulnérabilité critique vient d'être découverte dans le populaire plugin WordPress* ***"Email Subscribers by Icegram Express - Email Marketing, Newsletters, Automation for WordPress & WooCommerce".*** *Le plugin WordPress* ***"Email Subscribers by Icegram Express"*** *est un outil populaire servant à gérer les abonnements par e-mail, envoyer des newsletters, et automatiser les campagnes de marketing par e-mail sur des sites WordPress et WooCommerce.* *La vulnérabilité identifiée sous* ***CVE-2024-6172****, a un score de criticité 9.8 sur 10 indiquant son impact sévère sur les sites WordPress vulnérables. Elle provient d'un échappement insuffisant du paramètre* ***db*** *fourni par l'utilisateur et d'une préparation inadéquate sur une requête SQL existante.* *Une exploitation réussie de cette vulnérabilité sur les systèmes vulnérables entraine des impacts importants :* • *Elle permet à des attaquants non authentifiés d'exécuter des attaques d'injection SQL programmées, ce qui leur permet d'ajouter des requêtes SQL supplémentaires aux requêtes existantes ;* • *Les attaquants peuvent extraire des informations sensibles de la base de données, ce qui représente un risque important pour la sécurité et la confidentialité des sites web concernés ;*

	• *Les sites web qui utilisent ce plugin risquent de subir des violations de données, qui pourraient révéler des informations sensibles sur les utilisateurs, notamment des adresses électroniques, des mots de passe et d'autres données personnelles.*
Solutions	*Tout administrateur de sites web WordPress utilisant le plugin* ***"Email Subscribers by Icegram Express"*** *doit réduire immédiatement ce risque en appliquant les mesures de rémédiation suivantes:* • ***Mettre à jour le plugin:*** *passer urgemment à la version* ***5.7.26****, ou une version corrigée plus récente;* • ***Désactiver le plugin "Email Subscribers by Icegram Express":*** *si une mise à jour n'est pas disponible pour vous, envisagez de désactiver temporairement le plugin afin d'éviter toute exploitation potentielle;* • ***Surveiller les activités inhabituelles:*** *vérifiez que votre site web ne présente aucun signe d'activité inhabituelle, comme des requêtes de base de données inattendues ou des tentatives d'accès non autorisé;* • ***Sauvegarde des données :*** *sauvegardez régulièrement les données de votre site web afin de pouvoir les restaurer en cas de violation de la sécurité.*
Liens pour plus de détails	https://plugins.trac.wordpress.org/changeset/3107964/email-subscribers#file4 https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/email-subscribers/email-subscribers-by-icegram-express-email-marketing-newsletters-automation-for-wordpress-woocommerce-5725-unauthenticated-sql-injection-via-unsubscribe https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/email-subscribers