ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité
des Systèmes d'Information

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات

BULLETIN DE SECURITE

Titre	Vulnérabilité dans wolfSSH
Numéro de Référence	59830801/26
Date de Publication	08 Janvier 2026
Risque	Important
Impact	Important

Systèmes affectés

- wolfSSH version 1.4.21 et antérieures

Identificateurs externes

- CVE-2025-14942

Bilan de la vulnérabilité

Une vulnérabilité affecte le mécanisme d'échange de clés de wolfSSH, qui peut être exploité par un attaquant pour altérer le déroulement normal de la négociation SSH. En manipulant l'ordre et le contenu des messages échangés, un attaquant peut amener le client à transmettre son mot de passe en clair, à générer et envoyer une signature cryptographique invalide, ou encore à ignorer entièrement l'étape d'authentification utilisateur.

Solution :

Veuillez se référer au bulletin de sécurité wolfSSH pour plus d'infirmation.

Risque :

- Contournement de la politique de sécurité ;
- Atteinte à la confidentialité des données ;
- Atteinte à l'intégrité des données ;

Annexe

Bulletin de sécurité wolfSSH**:**

- https://github.com/wolfSSL/wolfssh/pull/855

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات, مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma