



NOTE DE SECURITE

Titre	L'attaque « Terrapin » cible les clients et serveurs SSH
Numéro de Référence	45390401/24
Date de Publication	04 Janvier 2024
Risque	Critique
Impact	Critique

Une attaque sophistiquée appelée "Terrapin" exploite la vulnérabilité critique « CVE-2023-48795 » dans le protocole Secure Shell. Cette vulnérabilité permet aux attaquants de réduire la sécurité d'une connexion SSH établie, ce qui peut conduire à un accès non autorisé, à l'exfiltration de données et même au déploiement de logiciels malveillants. Cette vulnérabilité affecte un large éventail de versions de logiciels clients et serveurs SSH, y compris les versions d'OpenSSH antérieures à 9.6. Les administrateurs peuvent également utiliser le scanner de vulnérabilité Terrapin pour déterminer si un client ou un serveur SSH est vulnérable. Pour une liste complète des implémentations affectées connues, voir <https://terrapin-attack.com/patches.html>

Recommandations :

- Appliquez les correctifs de sécurité du fournisseur de logiciels dès que possible. Cela implique généralement de passer à la dernière version de votre client SSH et de votre logiciel serveur.
- Envisagez de désactiver les algorithmes non sécurisés de chiffrement et d'échange de clés dans la configuration du serveur SSH.
- Surveillez les activités suspectes sur les systèmes SSH, telle que des tentatives de connexion inattendues ou des changements de configuration.
- Utilisez des mots de passe forts et uniques pour tous les comptes SSH et activer l'authentification à deux facteurs dans la mesure du possible.

Référence :

Terrapin Attack

- <https://terrapin-attack.com/patches.html>

Bulletin de sécurité maCERT du 20 Décembre 2023:

- <https://www.dgssi.gov.ma/fr/bulletins/vulnerabilites-dans-openssh>