

Faille 1 :

node-tar :

- Arbitrary File Overwrite : permet aux attaquants d'écrire ou de créer des fichiers à des endroits arbitraires sur le serveur, ce qui peut leur permettre d'exécuter du code malveillant ou de modifier des fichiers de configuration.
- Symlink Poisoning : Permet aux attaquants de créer d'avoir accès à des chemins absous sur le système

Solution : le problème venant de node-tar qui est une dépendance de sqlite, la meilleure solution serait de mettre sqlite à jour, la faille ayant été corrigée dans les versions plus récentes.

Faille 2 :

Token d'authentification en dur dans le code. Risque de sécurité au niveau de l'authentification.

Solution : Créer un .env pour stocker les variables d'environnement.

Faille 3 :

Adresse IP de l'api en dur dans le code et visible dans une erreur sur une route non protégée. Accès direct à la base de données en cas de récupération du code.

Solution : Pareil que pour la faille précédente.

Faille 4 :

Mauvais typage de données dans la création de la table (ligne 14 fichier server.js)

Solution : username et password devraient être des CHAR ou VARCHAR, et role devrait soit être un CHAR/VARCHAR avec une contrainte CHECK de validation, ou une énumération contenant uniquement les rôles autorisés.

Faille 5 :

L'endpoint get remonte l'id et le rôle de l'utilisateur alors qu'elles devraient rester des informations confidentielles.

Solution : Utiliser un token avec les informations nécessaires