Rapport de Scan CVE

# Services

Service: ssh, Version: 9.3

Description: Le service SSH (Secure Shell) est un protocole sécurisé utilisé pour établir une connexion chiffrée entre deux ordinateurs, permettant ainsi de transférer des données de manière sécurisée sur un réseau. Il est couramment utilisé pour accéder à distance à des serveurs ou des systèmes informatiques en toute sécurité.

Service: domain, Version:

Description: Le service de domaine est un service informatique qui permet de gérer et de contrôler les noms de domaine sur Internet. Il permet d'associer des adresses IP à des noms de domaine, facilitant ainsi l'accès aux sites web et aux applications en ligne.

Service: http, Version:

Description: HTTP (Hypertext Transfer Protocol) est un protocole de communication utilisé pour transférer des données sur le web. Il permet d'échanger des informations entre un navigateur web et un serveur web, facilitant ainsi l'accès aux sites internet, le partage de contenus et l'interaction en ligne.

# Vulnérabilités

## Service: domain (Version: )

**CVE ID: CVE-2023-7025**Description: Le CVE-2023-7025 est une vulnérabilité de type exécution de code à distance (RCE) affectant les serveurs web Apache Tomcat versions 7 à 10. Cette faille permet à un attaquant distant d'exécuter du code malveillant sur le serveur ciblé, compromettant ainsi la confidentialité et l'intégrité des données. Il est recommandé de mettre à jour vers une version patchée dès que possible pour atténuer ce risque.  
*Recommandation: La CVE-2023-7025 est une vulnérabilité critique qui peut être mitigée en appliquant immédiatement les correctifs de sécurité fournis par le fournisseur de logiciels. Il est également recommandé de limiter l'accès aux ressources sensibles et de surveiller attentivement tout comportement suspect sur le réseau. Enfin, sensibiliser les utilisateurs aux pratiques de sécurité informatique et mettre en place une politique de gestion des correctifs régulière sont des mesures préventives essentielles.*