KEYSTONE.

USTHB

21/06/2025

Nom du projet : Soutenance

ID du scan : 6857386aa44a6c11d3dfdb5c

IP cible : 192.168.31.129

Date : 21/06/2025

RÉSULTATS

Port	Technologie	Version	Vulnérable	CVE	Criticité
80	http	Apache httpd 2.4.29 ((Ubuntu))	False	—	—
1335	http	Apache httpd 2.4.25 ((Debian))	False	—	—
1336	http	Apache httpd 2.4.7 ((Ubuntu))	False	—	—
1337	http	Apache Tomcat/Coyote JSP engine 1.1	False	—	—
3000	ppp?	N/A	False	—	—
8080	http	Apache httpd 2.4.7 ((Ubuntu))	False	—	—

RECOMMANDATIONS

1 - Risques potentiels :
- Exposition de services web différents sur des ports différents
- Utilisation de versions différentes d'Apache et Tomcat
- Utilisation de versions obsolètes d'Apache (2.4.25 et 2.4.7)
- Port 3000 avec service inconnu

2 - Mesures de sécurité préventives :
- Mettre à jour les versions d'Apache et Tomcat
- Limiter l'exposition des services web à des ports nécessaires
- Configurer les firewalls pour bloquer les ports non nécessaires
- Utiliser des stratégies de sécurité web pour les services web (comme les directives d'Apache)
- Identifier le service sur le port 3000 et appliquer les mesures de sécurité appropriées