KEYSTONE.

USTHB

21/06/2025

Nom du projet : Soutenance

ID du scan : 6857340ca44a6c11d3dfdb5b

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 :
- Exposure aux vulnérabilités connues des versions Apache httpd 2.4.29, 2.4.25, 2.4.7 et Tomcat/Coyote JSP engine 1.1
- Risque de DDoS (attaque de déni de service) sur les ports 80 et 8080

2 - Mesures de sécurité préventives :
- Mise à jour des versions Apache httpd et Tomcat
- Configuration de la sécurité des applications web (ex : limiter les extensions autorisées, désactiver les fonctionnalités inutiles)
- Configuration de la sécurité du serveur (ex : limiter le nombre de connexions simultanées, activer les logs détaillés)
- Configuration de la sécurité du réseau (ex : filtrage des paquets, blocage des adresses IP suspectes)
- Configuration de la sécurité des applications (ex : utilisation de frameworks de sécurité, validation des entrées utilisateur)