Logo Keystone

CEVITAL

15/06/2025

Nom du projet : CEVITAL

ID du scan : 684f4dbe78d9c8f74453f866

IP cible : 192.168.31.129

Date : 15/06/2025

RÉSULTATS

Port	Technologie	Version	Vulnérable	CVE	Criticité
80	http	Apache httpd 2.4.29 ((Ubuntu))	True	CVE-2017-15710, CVE-2017-15715, CVE-2018-1303	**Haute**

RECOMMANDATIONS

CVE-2017-15710 :
- Description : Vulnérabilité de type Cross-Site Scripting (XSS) dans le service HTTP sur le port 80
- Recommandation : Mettre en place des contrôles de validation rigoureux pour les entrées utilisateur et des mécanismes de protection contre les attaques XSS

CVE-2017-15715 :
- Description : Vulnérabilité de type Injection SQL dans le service HTTP sur le port 80
- Recommandation : Mettre en place des contrôles de validation rigoureux pour les entrées utilisateur et des préparations de chaînes SQL pour éviter les attaques d'injection SQL

CVE-2018-1303 :
- Description : Vulnérabilité de type Remote Code Execution (RCE) dans le service HTTP sur le port 80
- Recommandation : Mettre à jour le logiciel concerné pour résoudre la vulnérabilité et appliquer des stratégies de sécurité pour empêcher les attaques RCE, telles que les pare-feu et les contrôles d'accès restrictifs