

**Nom du projet :** Soutenance**ID du scan :** 68573b2bd6c889d990bd5db2**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))	True	CVE-2017-15710, CVE-2017-15715, CVE-2018-1303	Haute
1335	http	Apache httpd 2.4.25 ((Debian))	True	CVE-2017-3167, CVE-2017-3169, CVE-2017-7668	Haute
1336	http	Apache httpd 2.4.7 ((Ubuntu))	True	CVE-2016-5387, CVE-2017-3167, CVE-2017-7679	Haute
1337	http	Apache Tomcat/Coyote JSP engine 1.1	True	CVE-2004-0174, CVE-2017-9788, CVE-2017-9798	Haute
3000	ppp?	N/A	False	—	—
8080	http	Apache httpd 2.4.7 ((Ubuntu))	True	CVE-2016-5387, CVE-2017-3167, CVE-2017-7679	Haute

## RECOMMANDATIONS

**CVE-2017-15710 :**

- Description : Dans Apache httpd 2.0.23 à 2.0.65, 2.2.0 à 2.2.34, et 2.4.0 à 2.4.29, mod\_authnz\_ldap, si configuré avec AuthLDAPCharsetConfig, utilise la valeur de l'entête Accept-Language pour rechercher l'encodage de caractère correct lors de la vérification des informations d'identification de l'utilisateur. Si la valeur de l'entête n'est pas présente dans la table de conversion des caractères, un mécanisme de redémarrage rapide est utilisé pour tronquer la valeur à deux caractères. Une valeur de moins de deux caractères entraîne une écriture hors limites d'un byte NUL dans une mémoire non liée à la chaîne. Dans le pire des cas, cela

peut entraîner une panne du processus, qui peut être utilisée comme attaque Denial of Service. Dans le cas le plus probable, cette mémoire est déjà réservée pour une utilisation ultérieure et l'effet n'est pas visible.

- Recommandation : Mettez à jour Apache httpd pour éviter cette vulnérabilité.

CVE-2017-15715 :

- Description : Dans Apache httpd 2.4.0 à 2.4.29, l'expression spécifiée dans `File` peut correspondre à '\$' à un caractère de saut de ligne dans un nom de fichier malicieux, plutôt que de correspondre uniquement à la fin du nom de fichier. Cela peut être exploité dans des environnements où les téléchargements de certains fichiers sont bloqués de manière externe, mais uniquement en bloquant la partie finale du nom de fichier.

- Recommandation : Mettez à jour Apache httpd pour éviter cette vulnérabilité.

CVE-2018-1303 :

- Description : Une demande HTTP spécialement conçue peut avoir fait chuter le serveur Apache HTTP avant la version 2.4.30 en raison d'une lecture hors limites dans la préparation de données à être stockées dans la mémoire partagée. Cela peut être utilisé comme attaque Denial of Service contre les utilisateurs de `mod_cache_socache`. La vulnérabilité est considérée comme à faible risque car `mod_cache_socache` n'est pas largement utilisé et `mod_cache_disk` n'est pas concerné par cette vulnérabilité.

- Recommandation : Mettez à jour Apache httpd pour éviter cette vulnérabilité.

CVE-2017-3167 :

- Description : Dans Apache httpd 2.2.x avant 2.2.33 et 2.4.x avant 2.4.26, l'utilisation de `ap_get_basic_auth_pw()` par des modules tiers en dehors de la phase d'authentification peut entraîner l'évitement des exigences d'authentification.

- Recommandation : Mettez à jour Apache httpd pour éviter cette vulnérabilité.

CVE-2