KEYSTONE.

USTHB

21/06/2025

Nom du projet : Soutenance

ID du scan : 685708efd42d8a5b680afe89

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**

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 approprié lors de la vérification des identifiants d'utilisateur. Si la valeur de l'entête n'est pas présente dans la table de conversion de caractères, un mécanisme de redémarrage est utilisé pour tronquer le nombre de caractères à deux. Si le nombre de caractères est inférieur à deux, cela entraîne une écriture hors limites d'un octet NUL dans une mémoire non liée à la chaîne. Dans le pire des cas, cela pourrait provoquer une panne du processus, ce qui peut être utilisé comme attaque de déni de service. Dans le cas plus probable, cette mémoire est déjà réservée pour une utilisation ultérieure et l'issue n'a aucun effet.
- Recommandation : Mettez à jour Apache httpd pour la version la plus récente qui n'est pas vulnérable à cette faille. Si cela n'est pas possible, vous pouvez limiter l'accès aux ressources vulnérables en utilisant des stratégies de sécurité supplémentaires telles que des règles de pare-feu ou des restrictions de l'accès aux fichiers.

CVE-2017-15715 :
- Description : Dans Apache httpd 2.4.0 à 2.4.29, l'expression spécifiée dans peut correspondre à '$' à un caractère de saut de ligne dans un nom de fichier malveillant, 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 à l'extérieur, mais seulement en bloquant la partie finale du nom de fichier.
- Recommandation : Mettez à jour Apache httpd pour la version la plus récente qui n'est pas vulnérable à cette faille. Si cela n'est pas possible, vous pouvez limiter l'accès aux ressources vulnérables en utilisant des stratégies de sécurité supplémentaires telles que des règles de pare-feu ou des restrictions de l'accès aux fichiers.

CVE-2018-1303 :
- Description : Une demande HTTP spécialement conçue peut avoir provoqué une panne de l'Apache HTTP Server 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 de déni de service contre les utilisateurs de mod_cache_socache. La vulnérabilité est considérée comme à faible risque car mod_cache_socache n'est pas utilisé couramment, mod_cache_disk n'est pas concerné par cette