KEYSTONE.

test

21/06/2025

Nom du projet : Soutenance

ID du scan : 6856f73f1ca89d721511ff68

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'en-tête Accept-Language pour rechercher l'encodage de caractère correct lors de la vérification des identifiants d'utilisateur. Si la valeur de l'en-tête n'est pas présente dans la table de conversion de charset, un mécanisme de redémarrage est utilisé pour tronquer la valeur à deux caractères afin de permettre un redémarrage rapide (par exemple, 'en-US' est tronqué à 'en'). Une valeur d'en-tête inférieure à deux caractères force une écriture hors limites d'un octet NUL dans une mémoire non liée à la chaîne. Dans le pire des cas, l'exécution du processus pourrait être interrompue, ce qui pourrait être utilisé pour lancer une 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 : Mettre à jour Apache httpd pour la version la plus récente qui n'est pas vulnérable à cette faille.

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 pourrait être exploité dans des environnements où les uploads de certains fichiers sont bloqués de manière externe, mais uniquement en bloquant la partie finale du nom de fichier.
- Recommandation : Mettre à jour Apache httpd pour la version la plus récente qui n'est pas vulnérable à cette faille.

CVE-2018-1303 :
- Description : Une requête HTTP spécialement conçue pourrait avoir fait tomber l'Apache HTTP Server avant la version 2.4.30 en raison d'une lecture hors limites d'une donnée lors de la préparation des données à être stockées dans la mémoire partagée. Cela pourrait être utilisé pour lancer une 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 largement utilisé, mod_cache_disk n'est pas concerné par cette vulnérabilité.
- Recommandation : Mettre à jour Apache httpd pour la version la plus récente qui n'est pas vulnérable à cette faille.