KEYSTONE.

test

21/06/2025

Nom du projet : Soutenance

ID du scan : 6856f8851ca89d721511ff69

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 caractères 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 caractères, un mécanisme de reprise est utilisé pour couper la valeur à deux caractères pour permettre un essai rapide (par exemple, 'en-US' est coupé à 'en'). Une valeur d'en-tête de moins de deux caractères force une écriture hors limite d'un octet NUL dans une mémoire non liée à la chaîne. Dans le pire des cas, le processus pourrait s'arrêter, ce qui pourrait 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 contient une correction de la vulnérabilité. Si cela n'est pas possible, limitez l'accès à la zone concernée et appliquez des stratégies de sécurité supplémentaires pour réduire les risques d'exploitation de la vulnérabilité.

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 extérieurement, mais uniquement en bloquant la partie finale du nom de fichier.
- Recommandation : Mettez à jour Apache httpd pour la version la plus récente qui contient une correction de la vulnérabilité. Si cela n'est pas possible, appliquez des stratégies de sécurité supplémentaires pour réduire les risques d'exploitation de la vulnérabilité, telles que des règles de sécurité plus restrictives pour les noms de fichiers.

CVE-2018-1303 :
- Description : Une demande HTTP spécialement conçue peut avoir fait s'arrêter le serveur Apache HTTP avant la version 2.4.30 en raison d'une lecture hors limite d'un octet lors de la préparation de données à être stockées dans la mémoire partagée. Cela pourrait 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