KEYSTONE.

USTHB

21/06/2025

Nom du projet : Soutenance

ID du scan : 685703181ca89d721511ff6c

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 caractères 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 de 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 utilisée. Dans le pire des cas, cela peut

entraîner une panne de processus, ce qui peut être utilisé pour effectuer une attaque de déni de service. Dans le cas le plus probable, cette mémoire est déjà réservée pour une utilisation ultérieure et l'effet n'est pas visible.
- Recommandation : Mettre à jour Apache httpd pour la version la plus récente qui contient une correction de cette 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 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 : Mettre à jour Apache httpd pour la version la plus récente qui contient une correction de cette vulnérabilité.

CVE-2018-1303 :
- Description : Une demande HTTP spécialement conçue peut avoir provoqué une lecture hors limites dans le serveur HTTP Apache avant la version 2.4.30 en préparant les données à être stockées dans la mémoire partagée. Cela peut être utilisé pour effectuer 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 contient une correction de 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'