KEYSTONE.

Rapport d'énumération automatisée

21/06/2025

Nom du projet : usthb

ID du scan : 001

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 : In Apache httpd 2.0.23 to 2.0.65, 2.2.0 to 2.2.34, and 2.4.0 to 2.4.29, mod_authnz_ldap, if configured with AuthLDAPCharsetConfig, uses the Accept-Language header value to lookup the right charset encoding when verifying the user's credentials. If the header value is not present in the charset conversion table, a fallback mechanism is used to truncate it to a two characters value to allow a quick retry (for example, 'en-US' is truncated to 'en'). A header value of less than two characters forces an out of bound write of one NUL byte to a memory location that is not part of the string. In the worst case, quite unlikely, the process would crash which could be used as a Denial of Service attack. In the more likely case, this memory is already reserved for future use and the issue has no effect at all.
- Recommandation : Upgrade Apache httpd to a version that is not affected by this vulnerability (2.4.30 or higher) or configure mod_authnz_ldap to not use AuthLDAPCharsetConfig.

CVE-2017-15715 :
- Description : In Apache httpd 2.4.0 to 2.4.29, the expression specified in could match '$' to a newline character in a malicious filename, rather than matching only the end of the filename. This could be exploited in environments where uploads of some files are are externally blocked, but only by matching the trailing portion of the filename.
- Recommandation : Upgrade Apache httpd to a version that is not affected by this vulnerability (2.4.30 or higher) or modify the expression to ensure it only matches the end of the filename.

CVE-2018-1303 :
- Description : A specially crafted HTTP request header could have crashed the Apache HTTP Server prior to version 2.4.30 due to an out of bound read while preparing data to be cached in shared memory. It could be used as a Denial of Service attack against users of mod_cache_socache. The vulnerability is considered as low risk since mod_cache_socache is not widely used, mod_cache_disk is not concerned by this vulnerability.
- Recommandation : Upgrade Apache httpd to a version that is not affected by this vulnerability (2.4.30 or higher) or disable mod_cache_socache if it is not necessary.