# CVE Detail – CVE-2012-6707

WordPress through 4.8.2 uses a weak MD5-based password hashing algorithm, which makes it easier for attackers to determine cleartext values by leveraging access to the hash values. NOTE: the approach to changing this may not be fully compatible with certain use cases, such as migration of a WordPress site from a web host that uses a recent PHP version to a different web host that uses PHP 5.2. These use cases are plausible (but very unlikely) based on statistics showing widespread deployment of WordPress with obsolete PHP versions.

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## EPSS

EPSS Score: N/A

Percentile: 0.40274

## CVSS Scoring

CVSS v3.0 Score: 7.5

Severity: HIGH

## Mapped CWE(s)

* CWE-326: Inadequate Encryption Strength

## CAPEC(s)

* CAPEC-112: Brute Force
* CAPEC-192: Protocol Analysis
* CAPEC-20: Encryption Brute Forcing

## ATT&CK Techniques

* T1110: Brute Force

## Used By (Actors/Tools)

* Chaos (malware)
* Caterpillar WebShell (malware)
* Pysa (malware)
* Kinsing (malware)
* QakBot (malware)
* PoshC2 (tool)
* CrackMapExec (tool)
* Dragonfly (intrusion-set)
* OilRig (intrusion-set)
* Fox Kitten (intrusion-set)
* Turla (intrusion-set)
* Ember Bear (intrusion-set)
* APT28 (intrusion-set)
* HEXANE (intrusion-set)
* 2016 Ukraine Electric Power Attack (campaign)
* APT39 (intrusion-set)
* APT38 (intrusion-set)
* Operation Dream Job (campaign)
* DarkVishnya (intrusion-set)
* APT41 (intrusion-set)
* Agrius (intrusion-set)
* FIN5 (intrusion-set)

## Affected Products

* cpe:2.3:a:wordpress:wordpress:\*:\*:\*:\*:\*:\*:\*:\*