# CVE Detail – CVE-2022-4036

The Appointment Hour Booking plugin for WordPress is vulnerable to CAPTCHA bypass in versions up to, and including, 1.3.72. This is due to the use of insufficiently strong hashing algorithm on the CAPTCHA secret that is also displayed to the user via a cookie.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.06644

## CVSS Scoring

CVSS v3.1 Score: 5.3

Severity: MEDIUM

## 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:dwbooster:appointment\_hour\_booking:\*:\*:\*:\*:\*:wordpress:\*:\*