

Forum:[Hack Forums](#)

Thread: [the wordpress DoS vulnerability](#)

itzRealWubaDubaLubb - November 27, 2024, 2:23 pm

WordPress is a popular open-source content management system (CMS) that powers over 43% of the web. Due to its user-friendly interface and wide range of plugins, it is widely used by individuals and small businesses.

The wp-cron.php file, located in the root directory of a WordPress website, is a virtual cron job that automates processes like core updates, plugin updates, scheduled posts, and more. However, sending mass requests to this file can result in a denial-of-service (DoS) attack if not properly configured.

How to find it: To find the wp-cron.php file, you can verify if the target website uses WordPress by using a tool called Wappalyzer. This extension will identify the technologies used by the site and help you identify if it's a WordPress site.

After verifying that the site is using WordPress, you can enter "/wp-cron.php" after the URL of the target site. If the site shows a blank white page, that means the wp-cron.php file is exposed.

You can also send a curl request to the target site to check the HTTP status code. If it's 200, the wp-cron.php file is found.

How to exploit it: To exploit the vulnerability, you can use a tool called doser.go, which is a simple script written in Go that sends a large number of requests to the wp-cron.php file.

Installing doser.go:
go build doser.go

Sending mass requests to wp-cron.php:

```
./doser -t 9999 -g 'https:**target.com*wp-cron.php'
```

Monitoring the site's behavior: After sending the requests, you should reload the site and observe its performance. If the site becomes slow or unresponsive, it indicates that the site is vulnerable to uncontrolled resource consumption through the misconfiguration of wp-cron.php.

Impact: If successful, this misconfiguration can lead to denial-of-service (DoS) attacks, server overload, increased resource usage, and potential data loss or downtime of the site.