MODULE

Wordpress Work The Flow Upload Vulnerability

← BACK TO SEARCH

Disclosed
Mar 14, 2015

Created
May 30, 2018

Description

This module exploits an arbitrary PHP code upload in the WordPress Work The Flow plugin, version 2.5.2. The vulnerability allows for arbitrary file upload and remote code execution.

Authors

Claudio Viviani
Roberto Soares Espreto robertoespreto@gmail.com

Platform

PHP

Architectures

php

References

Source Code

History

Module Options

To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

```
msf > use exploit/unix/webapp/wp_worktheflow_upload
msf exploit(wp_worktheflow_upload) > show targets
    ...targets...
msf exploit(wp_worktheflow_upload) > set TARGET < target-id >
msf exploit(wp_worktheflow_upload) > show options
    ...show and set options...
msf exploit(wp_worktheflow_upload) > exploit
```

Emergent Threat Response

Webinars & Events

Rapid7 Labs Research

Vulnerability Database

Security Fundamentals

FOR CUSTOMERS

Sign In

Support Portal

Product Documentation

Extension Library

Rapid7 Academy

Customer Escalation Portal

CONTACT SUPPORT

+1-866-390-8113

FOLLOW US

LinkedIn

X (Twitter)

Facebook

Instagram

Bluesky