WordPress Responsive Thumbnail Slider 1.0 Shell Upload

2015.08.28

Credit: **Arash Khazaei (https://cxsecurity.com/author/Arash+Khazaei/1/)**

Risk: **High**

Local: **No**

Remote: **Yes**

CVE: **N/A**

CWE: **CWE-264 (https://cxsecurity.com/cwe/CWE-264)**

```
<!--
# Exploit Title: Wordpress Responsive Thumbnail Slider Arbitrary F
ile Upload
# Date: 2015/8/29
# Exploit Author: Arash Khazaei
# Vendor Homepage:
https://wordpress.org/plugins/wp-responsive-thumbnail-slider/
# Software Link:
https://downloads.wordpress.org/plugin/wp-responsive-thumbnail-sli
der.zip
# Version: 1.0
# Tested on: Kali , Iceweasel Browser
# CVE : N/A
# Contact : http://twitter.com/0xClay
# Email : 0xclay@gmail.com
# Site : http://bhunter.ir

# Intrduction :

# Wordpress Responsive Thumbnail Slider Plugin iS A With 6000+ Act
ive
Install
# And Suffer From A File Upload Vulnerability Allow Attacker Uploa
```

```
d Shell
As A Image .
# Authors , Editors And Of Course Administrators This Vulnerabilit
y To Harm
WebSite .
-->
# POC :

# For Exploiting This Vulnerability :

# Go To Add Image Section And Upload File By Self Plugin Uploader
# Then Upload File With Double Extension Image
# And By Using A BurpSuite Or Tamper Data Change The File Name Fro
m
Shell.php.jpg To Shell.php
# And Shell Is Uploaded . :)



<!-- Discovered By Arash Khazaei (Aka JunkyBoy) -->
```

References:

https://downloads.wordpress.org/plugin/wp-responsive-thumbnail-slider.zip

See this note in RAW Version (https://cxsecurity.com/ascii/WLB-2015080170)

Post

Vote for this issue: 1 0

100%

Comment it here.

Nick (*)

Nick

Email (*)

Email

Video

Link to Youtube

Text (*)