

[UNIX] Open Motif Multiple Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-01/msg00051.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 16 Jan 2006 10:06:16 +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>

Open Motif Multiple Buffer Overflow

SUMMARY

"Open Motif provides libraries which implement the Motif graphical user interface on Unix-based operating systems. "

Lack of proper input and length validation allows attackers to execute arbitrary code to an Open Motif programs.

DETAILS

Vulnerable Systems:

* Open Motif version 2.2.3 and prior

Open Motif does not validate user and programs input when using the `diag_issue_diagnostic()` function allowing attackers to execute arbitrary code using a bigger value then can be contained at buffer.

Vulnerable Code:

Clients/ui/UiDiags.c

`diag_issue_diagnostic()`

202 void `diag_issue_diagnostic`

203 (int `d_message_number`, `src_source_record_type` *`az_src_rec`,

[UNIX] Open Motif Multiple Buffer Overflow

```
204 int l_start_column, ...)
205
206 {
207 va_list ap; /* ptr to variable length parameter */
208 int severity; /* severity of message */
209 int message_number; /* message number */
210 char msg_buffer[132]; /* buffer to construct message */
211 char ptr_buffer[buf_size]; /* buffer to construct pointer */
212 char loc_buffer[132]; /* buffer to construct location */
213 char src_buffer[buf_size]; /* buffer to hold source line */
.....
293 va_start(ap, l_start_column);
294
295 #ifndef NO_MESSAGE_CATALOG
296[1.1] vsprintf( msg_buffer,
297 catgets(uil_catd, UIL_SET1, msg_cat_table[message_number ],
298 diag_rz_msg_table[ message_number ].ac_text),
299 ap );
300 #else
301[1.2] vsprintf( msg_buffer,
302 diag_rz_msg_table[ message_number ].ac_text,
303 ap );
304 #endif
305 va_end(ap);
```

[1.1][1.2] call vsprintf will cause buffer overflow if ap is user-support data,so if one local or remote application which used this library may cause execute arbitrary code .

The use of user input of file name in the function open_source_file also vulnerable to buffer overflow, due the fact the strcpy is used without verifying that the value length of the parameter c_file_name is up to 256.

Vulnerable Code:

Clients/uil/UilSrcSrc.c

```
620 status
621 open_source_file( XmConst char *c_file_name,
622 uil_fcb_type *az_fcb,
623 src_source_buffer_type *az_source_buffer )
624 {
625
626 static unsigned short main_dir_len = 0;
627 boolean main_file;
628 int i; /* loop index through include files */
629 char buffer[256];
630
631
632 /* place the file name in the expanded_name buffer */
633
634 strcpy(buffer, c_file_name);
635
```

[UNIX] Open Motif Multiple Buffer Overflow

```
636 /* Determine if this is the main file or an include file. */
637
638 main_file = (main_fcb == NULL);
639
```

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3964>>
CVE-2005-3964

ADDITIONAL INFORMATION

The information has been provided by xforce.

The original article can be found at:

<<http://xforce.iss.net/xforce/xfdb/23388>>

<http://xforce.iss.net/xforce/xfdb/23388>,

<<http://archives.neohapsis.com/archives/fulldisclosure/2005-12/0047.html>>

<http://archives.neohapsis.com/archives/fulldisclosure/2005-12/0047.html>

Gentoo bug report:

<<http://www.gentoo.org/security/en/glsa/glsa-200512-16.xml>>

<http://www.gentoo.org/security/en/glsa/glsa-200512-16.xml>

=====

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@xxxxxxxxxxxxxxxxx

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

=====

=====

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: [**\[UNIX\] Xname Buffer Overflow**](#)
 - Next by Date: [**\[NT\] PHP for Windows create named pipe Buffer Overflow**](#)
 - Previous by thread: [**\[UNIX\] Xname Buffer Overflow**](#)
 - Next by thread: [**\[NT\] PHP for Windows create named pipe Buffer Overflow**](#)
 - Index(es):
 - ◆ [**Date**](#)
 - ◆ [**Thread**](#)