

[NEWS] Mutt menu_pad_string() Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-02/0029.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 02/12/04

To: list@securiteam.com

Date: 12 Feb 2004 11:12:29 +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>

Mutt menu_pad_string() Buffer Overflow

SUMMARY

Mutt has issued a fix for a buffer overflow that can be triggered by incoming messages. There are reports about SPAM that has actually triggered this problem and crashed mutt.

DETAILS

Vulnerable Systems:

- * Mutt version 1.4.1 and prior

Immune Systems:

- * Mutt version 1.4.2 and newer
- * Mutt version 1.3.28 (unstable)

Vendor response:

It is recommended that users of mutt versions prior to 1.4.2 upgrade to this version, or apply the patch included below.

Users of "unstable" mutt versions after 1.3.28 (including 1.5.*) do not need to upgrade, as this problem had been fixed in the unstable branch in February 2002; unfortunately, the fix was not backported before 1.4 was released.

Securiteam: [NEWS] Mutt menu_pad_string() Buffer Overflow

Patch:

Index: menu.c

```
=====
RCS file: /cvs/mutt/mutt/menu.c,v
retrieving revision 2.27.2.1
diff -u -r2.27.2.1 menu.c
--- menu.c 28 Jan 2002 10:18:50 -0000 2.27.2.1
+++ menu.c 11 Feb 2004 10:05:52 -0000
@@ -148,30 +148,13 @@
     menu->make_entry (s, l, menu, i);
 }

-void menu_pad_string (char *s, size_t l)
+void menu_pad_string (char *s, size_t n)
 {
- size_t n = mutt_strlen (s);
  int shift = option (OPTARROWCURSOR) ? 3 : 0;
-
- l--; /* save room for the terminal \0 */
- if (l > COLS - shift)
- l = COLS - shift;
+ int cols = COLS - shift;

- /* Let's just pad the string anyway ... */
- mutt_format_string (s, INT_MAX, l, l, 0, ' ', s, n, 1);
- return;
-
-#if !defined (HAVE_BKGDSET) && !defined (USE_SLANG_CURSES)
- /* we have to pad the string with blanks to the end of line */
- if (n < l)
- {
- while (n < l)
- s[n++] = ' ';
- s[n] = 0;
- }
- else
-#endif
- s[l] = 0;
+ mutt_format_string (s, n, cols, cols, 0, ' ', s, strlen (s), 1);
+ s[n - 1] = 0;
 }

void menu_redraw_full (MUTTMENU *menu)
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:roessler@does-not-exist.org>>
Thomas Roessler.

Securiteam: [NEWS] Mutt menu_pad_string() Buffer Overflow

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.

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