

git

index : emacs.git

master

switch

Emacs source repository

summary refs log tree **commit** diff

log msg search

author

Xi Lu <lx@shellcodes.org>

2023-10-10 22:20:05 +0800

committer

Stefan Kangas <stefankangas@gmail.com>

2024-01-10 22:16:24 +0100

commit

820f0793f0b46448928905552726c1f1b999062f

(patch)

tree

b6d7993f6b7e20f509ff0885d187b80e52ac239d

parent

093ecb2aca1fa6d00f212b2426ddb7601fdbcf2d

(diff)

diff options

context:

3

space:

include

mode:

unified

Fix man.el shell injection vulnerability

* lisp/man.el (Man-translate-references): Fix shell injection vulnerability. (Bug#66390)
* test/lisp/man-tests.el (man-tests-Man-translate-references): New test.

Diffstat

-rw-r--r--	lisp/man.el	6	
-rw-r--r--	test/lisp/man-tests.el	12	

2 files changed, 17 insertions, 1 deletions

```
diff --git a/lisp/man.el b/lisp/man.el
index 55cb9383bec..d96396483d3 100644
--- a/lisp/man.el
+++ b/lisp/man.el
@@ -761,7 +761,11 @@ and the `Man-section-translations-alist' variables).
   (setq name (match-string 2 ref)
         section (match-string 1 ref)))
   (if (string= name "")
-      ref
+      ; Return the reference as is
+      ;; see Bug#66390
+      (mapconcat 'identity
+                  (mapcar #'shell-quote-argument
+                          (split-string ref "\\s-+"))
+                  " ")
+      ; Return the reference as is
+      (if Man-downcase-section-letters-flag
+          (setq section (downcase section))
+          (while slist

diff --git a/test/lisp/man-tests.el b/test/lisp/man-tests.el
index 140482ee622..11f5f805e43 100644
--- a/test/lisp/man-tests.el
+++ b/test/lisp/man-tests.el
@@ -161,6 +161,18 @@ DESCRIPTION
   (let ((button (button-at (match-beginning 0))))
     (should (and button (eq 'Man-xref-header-file (button-type button))))))

+(ert-deftest man-tests-Man-translate-references ()
+  (should (equal (Man-translate-references "basename")
+                  "basename"))
+  (should (equal (Man-translate-references "basename(3)")
```

```
+      "3 basename"))
+ (should (equal (Man-translate-references "basename(3v)")
+      "3v basename"))
+ (should (equal (Man-translate-references ";id")
+      "\\;id"))
+ (should (equal (Man-translate-references "-k basename")
+      "-k basename")))
+
+ (provide 'man-tests)

;;; man-tests.el ends here
```

generated by cgkit v1.3 (git 2.53.0) at 2026-06-29 21:25:22 +0000