index : m17n/m17n-lib.git

m17n-lib

master switch

summary refs log tree commit diff

log msg search

author	Chamod Anuradha <chamodanu12@gmail.com>	2026-10-09 21:16:05 +0200
committer	Mike FABIAN <mfabian@redhat.com>	2026-10-10 10:29:56 +0200
commit	f3b85087f90189f91c04ba1b62c5f0b879ff2b20 (patch)	
tree	f09a8301780a376e4b5f3aa6a78ed1d4d1ce562f	
parent	fb077403b613829d9b906d5f04bfacb101e028e7 (diff)	

diff options

context: 3

space: include

mode: unified

fix "Unitialized buffer when UTF-8 lead byte is invalid"

Diffstat

-rw-r--r-- src/ChangeLog 5

-rw-r--r-- src/coding.c 4

2 files changed, 9 insertions, 0 deletions

```
diff --git a/src/ChangeLog b/src/ChangeLog
index 9d45865..02866aa 100644
--- a/src/ChangeLog
+++ b/src/ChangeLog
@@ -1,3 +1,8 @@
+2026-10-09  Chamod Anuradha <chamodanu12@gmail.com>
+
+       * coding.c (decode_coding_iso_2022):
+       Avoid uninitialized buffer on invalid UTF-8 lead bytes.
+
 2026-10-09  K. Handa  <handa@gnu.org>

        * plist.c (read_mtext_element): Avoid SIGSEGV on invalid utf-8 bytes.

diff --git a/src/coding.c b/src/coding.c
index 940e445..f8246c3 100644
--- a/src/coding.c
+++ b/src/coding.c
@@ -1585,6 +1585,10 @@ decode_coding_iso_2022 (const unsigned char *source, int src_bytes, MText *mt,
          int bytes = CHAR_BYTES_BY_HEAD (c1);
          int i;

+         if (bytes == 0) /* 0xFE or 0xFF: invalid UTF-8 lead byte */
+           {
+             goto invalid_byte;
+           }
          buf[0] = c1;
          for (i = 1; i < bytes; i++)
            {
```