



index : coreutils.git

master

switch

GNU coreutils

summary

refs

log

tree

commit

diff

log msg

search

author Pádraig Brady <P@draigBrady.com> 2026-04-28 20:33:10 +0100
 committer Pádraig Brady <P@draigBrady.com> 2026-04-29 13:16:43 +0100
 commit [b60a159fdc5bfcf9988d3a4cb6f53abe8ad5d35d](#) (patch)
 tree [f7f139bd69bacd6525e190584407d3749897a40c](#)
 parent [00cd91288cce5e781dbc750e85ef00a74bc49def](#) (diff)

diff options

context: 3

space: include

mode: unified

unexpand: fix heap overflow

* src/unexpand.c (unexpand): Use xmalloc() to gracefully handle overflow. Also use the runtime locale specific MB_CUR_MAX rather than the worst case MB_LEN_MAX.
 * tests/unexpand/mb.sh: Add a test case that fails in a default glibc build with either MB_CUR_MAX or MB_LEN_MAX.
 * NEWS: Mention the bug fix.
 Reported by Michał Majchrowicz.

Diffstat

```
-rw-r--r-- NEWS 3
-rw-r--r-- src/unexpand.c 2
-rwxr-xr-x tests/unexpand/mb.sh 8
```

3 files changed, 12 insertions, 1 deletions

diff --git a/NEWS b/NEWS

index d7dc61e46..8e041272e 100644

--- a/NEWS

+++ b/NEWS

@@ -12,6 +12,9 @@ GNU coreutils NEWS

standard output is fully buffered, e.g., when redirected to a file.
 [bug introduced in coreutils-9.10]

+ 'unexpand -t' no longer overflows a heap buffer, for tab values > SIZE_MAX/16.
 + [bug introduced in coreutils-9.11]
 +

'uniq -w' no longer overruns the read buffer in multibyte locales.
 [bug introduced in coreutils-9.5]

diff --git a/src/unexpand.c b/src/unexpand.c

index 3cbff1b12..c859c17a3 100644

--- a/src/unexpand.c

+++ b/src/unexpand.c

@@ -131,7 +131,7 @@ unexpand (void)

/* The worst case is a non-blank character, then one blank, then a tab stop, then MAX_COLUMN_WIDTH - 1 blanks, then a non-blank; so allocate MAX_COLUMN_WIDTH bytes to store the blanks. */

- pending_blank = xmalloc (max_column_width * sizeof (char) * MB_LEN_MAX);
 + pending_blank = xmalloc (max_column_width, MB_CUR_MAX);

```
while (true)
{
```

```
diff --git a/tests/unexpand/mb.sh b/tests/unexpand/mb.sh
index 76a267903..076a1c1ae 100755
--- a/tests/unexpand/mb.sh
+++ b/tests/unexpand/mb.sh
@@ -17,6 +17,7 @@
. "${srcdir=.}/tests/init.sh"; path_prepend_ ./src
print_ver_ unexpand printf
+getlimits_

test "$LOCALE_FR_UTF8" != none || skip_ "French UTF-8 locale not available"
export LC_ALL="$LOCALE_FR_UTF8"
@@ -161,4 +162,11 @@ EOF
unexpand -a ./in ./in > out || fail=1
compare exp out > /dev/null 2>&1 || fail=1

+# Ensure overflow is handed gracefully
+# coreutils v9.11 induced a buffer overflow with mb_mul=4 (or 16).
+for mb_mul in 4 6; do
+ printf '    \n' | unexpand -t $(expr $SIZE_MAX / $mb_mul + 1) 2>err; ret=$?
+ test "$ret" = 1 || test "$ret" = 0 || { cat err; fail=1; }
+done
+
Exit $fail
```

generated by cgkit v1.3 (git 2.53.0) at 2026-07-24 10:58:36 +0000