CVE-2017-7476

描述：Gnulib before 2017-04-26 has a heap-based buffer overflow with the TZ environment variable. The error is in the save\_abbr function in time\_rz.c.

软件：Gnulib

源码：lib/time\_rz.c

出现位置： 153-169行

关键源码：

while (strcmp (zone\_copy, zone) != 0)

{

if (! (\*zone\_copy || (zone\_copy == tz->abbrs && tz->tz\_is\_set)))

{

size\_t zone\_size = strlen (zone) + 1;

if (zone\_size < tz->abbrs + ABBR\_SIZE\_MIN - zone\_copy)

extend\_abbrs (zone\_copy, zone, zone\_size);

else

{

tz = tz->next = tzalloc (zone);

if (!tz)

return false;

tz->tz\_is\_set = 0;

zone\_copy = tz->abbrs;

}

break;

}