Stack-based Buffer Overflow in rtl_433 #2012

Closed **ZFeiXQ** opened this issue on Mar 17 · 1 comment

ZFeiXQ commented on Mar 17

Command

```
./rtl_433  -d0 -H5 -H20 -f 433.70M -f 433.80M -f 433.90M POC1
```

POC1.zip

ASAN

```
SUMMARY: AddressSanitizer: stack-buffer-overflow /home/zxq/CVE_testing/ASAN-
install/rtl_433/src/devices/acurite.c:1244 in acurite_00275rm_decode
Shadow bytes around the buggy address:
  0x100003f00c10: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x100003f00c20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x100003f00c30: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x100003f00c40: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x100003f00c50: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x100003f00c60: 00 00 00 00 00 00 00 00 00 00 00[04]f3 f3 f3 f3
  0x100003f00c70: f3 f3 f3 f3 f3 f3 f3 f3 f3 f3 f3 f3 f3 f3 f3 f3
  0x100003f00c80: f3 f3 f3 f3 f3 f3 f3 f3 f3 f3 f3 00 00 00 00 00
  0x100003f00c90: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x100003f00ca0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x100003f00cb0: 00 00 00 00 00 00 00 00 00 00 f1 f1 f1 f1 00 f2
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
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  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
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==3559329==ABORTING
```

zuckschwerdt closed this as completed in `3745548` on Mar 18

---

zuckschwerdt commented on Mar 18 — Collaborator

Thanks! This was introduced with `1a9b05c`. We want `array[len - 1]` and not just assume there is space for `array[len]` ;)

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants