protobuf-c / **protobuf-c** Public

Code · Issues 24 · Pull requests 11 · Actions · Projects · Wiki · ...

New issue

Jump to bottom

UndefinedBehaviorSanitizer: invalid left shift in protobuf-c.c:2086 #506

Closed **pietroborrello** opened this issue on Apr 29 · 1 comment

Milestone 1.4.1

pietroborrello commented on Apr 29

Describe the bug

UndefinedBehaviorSanitizer: invalid left shift in protobuf-c.c:2086

To Reproduce

Built protobuf-c using clang-10 according to the oss-fuzz script with `CXXFLAGS='-O1 -fsanitize=address -fsanitize=array-bounds,bool,builtin,enum,float-divide-by-zero,function,integer-divide-by-zero,null,object-size,return,returns-nonnull-attribute,shift,signed-integer-overflow,unreachable,vla-bound,vptr'`

commit: `f224ab2`

UBSAN Output

```
$ ./protobuf-c-fuzzer id:000003,sig:06,src:000024,time:945,op:havoc,rep:16,trial:4
INFO: Seed: 1244782513
INFO: Loaded 1 modules   (3433 inline 8-bit counters): 3433 [0x5b06c3, 0x5b142c),
INFO: Loaded 1 PC tables (3433 PCs): 3433 [0x5587f8,0x565e88),
protobuf-c-fuzzer: Running 1 inputs 1 time(s) each.
Running: id:000003,sig:06,src:000024,time:945,op:havoc,rep:16,trial:4
protobuf-c/protobuf-c.c:2086:29: runtime error: left shift of 65 by 25 places cannot be
represented in type 'int'
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior protobuf-c/protobuf-c.c:2086:29 in
Executed id:000003,sig:06,src:000024,time:945,op:havoc,rep:16,trial:4 in 1 ms
```

testcases that trigger the issue:
protobuf-c.zip

millert mentioned this issue on Jun 6

Only shift unsigned values to avoid implementation-specific behavior. #508

Merged

carnil commented on Jun 25

It looks that CVE-2022-33070 is associated with this issue.

👍 1

edmonds added this to the **1.4.1** milestone on Jul 10

edmonds closed this as completed on Jul 10

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

1.4.1

Development

No branches or pull requests

3 participants