Fatal error · out of memory

Loaded 4 minutes ago

REDO TASK DELETE

OVERVIEW

Crash State: `out of memory`
`wire.(*Type).load`
`state.(*decodeState).Load.func2`
`state.safely`

Crash Type:	Fatal error	Created:	Thu, Nov 18, 2021, 10:19 PM	Security:	NO
Crash Address:	---	Sanitizer:	address (ASAN)	Reliably Reproduces:	YES
Issue:	None	Platform:	linux		
Fuzzing Engine:	libFuzzer	Fuzz Target:	state_load_fuzz	Job Type:	gvisor_libfuzzer_asan
Project:	test-project				
Related:	Group 401				
Fixed:	NO				

Minimized Testcase: (23 B) Unminimized Testcase: (23 B) Re-upload Testcase: Build:

LAST TESTED REVISION	REGRESSION REVISION RANGE
1:1 (No component revisions found!)	NA

CRASH STACKTRACE

--- LAST TESTED STACKTRACE (77 LINES) ---

```
[Environment] ASAN_OPTIONS=exitcode=77
+----------------------------------------Release Build Stacktrace----------------------------------------+
Command: /clusterfuzz/run_bot/clusterfuzz/bot/builds/gvisor_libfuzzer_asan/custom/gvisor/state_load_fuzz -rss_limit_mb=2560 -timeout=60 -runs=100 /clusterfuzz/run_bot/clusterfuzz/bot/inputs/fuzzer-testcases/crash-b1f49ec073cea3594990465bb6ad5537294f6e3b
Time ran: 0.02354288101196289

INFO: Running with entropic power schedule (0xFF, 100).
INFO: Seed: 4189772842
INFO: 5162 Extra Counters
/clusterfuzz/run_bot/clusterfuzz/bot/builds/gvisor_libfuzzer_asan/custom/gvisor/state_load_fuzz: Running 1 inputs 100 time(s) each.
Running: /clusterfuzz/run_bot/clusterfuzz/bot/inputs/fuzzer-testcases/crash-b1f49ec073cea3594990465bb6ad5537294f6e3b
runtime: out of memory: cannot allocate 118738590367744-byte block (3866624 in use)
fatal error: out of memory

goroutine 17 [running, locked to thread]:
runtime.throw({0x64d1d3, 0x0})
 runtime/panic.go:1198 +0x71 fp=0x10c0000bc4d8 sp=0x10c0000bc4a8 pc=0x58fe71
runtime.(*mcache).allocLarge(0x7f7048bbc008, 0x6bfdfb5fefd0, 0x80, 0x0)
 runtime/mcache.go:229 +0x22e fp=0x10c0000bc538 sp=0x10c0000bc4d8 pc=0x57364e
runtime.mallocgc(0x6bfdfb5fefd0, 0x6b72e0, 0x1)
 runtime/malloc.go:1082 +0x5c5 fp=0x10c0000bc5b8 sp=0x10c0000bc538 pc=0x56aa05
runtime.makeslice(0x6d2320, 0x10c000116000, 0x7f70491405b8)
 runtime/slice.go:98 +0x52 fp=0x10c0000bc5e0 sp=0x10c0000bc5b8 pc=0x5a4a72
gvisor.dev/gvisor/pkg/state/wire.loadType({0x6d2320, 0x10c000116000})
 gvisor.dev/gvisor/pkg/state/wire/wire.go:675 +0x88 fp=0x10c0000bc658 sp=0x10c0000bc5e0 pc=0x61f9c8
gvisor.dev/gvisor/pkg/state/wire.(*Type).load(...)
 gvisor.dev/gvisor/pkg/state/wire/wire.go:699
gvisor.dev/gvisor/pkg/state/wire.Load({0x6d2320, 0x10c000116000})
 gvisor.dev/gvisor/pkg/state/wire/wire.go:951 +0x7a9 fp=0x10c0000bc778 sp=0x10c0000bc658 pc=0x6206a9
gvisor.dev/gvisor/pkg/state.(*decodeState).Load.func2()
 gvisor.dev/gvisor/pkg/state/decode.go:616 +0xbe fp=0x10c0000bc838 sp=0x10c0000bc778 pc=0x627bbe
gvisor.dev/gvisor/pkg/state.safely(0x6d2320)
 gvisor.dev/gvisor/pkg/state/state.go:321 +0x71 fp=0x10c0000bc878 sp=0x10c0000bc838 pc=0x629591
gvisor.dev/gvisor/pkg/state.(*decodeState).Load(0x10c000118000, {0x0, 0x0, 0x30})
 gvisor.dev/gvisor/pkg/state/decode.go:609 +0x445 fp=0x10c0000bcb68 sp=0x10c0000bc878 pc=0x626f25
gvisor.dev/gvisor/pkg/state.Load.func1()
 gvisor.dev/gvisor/pkg/state/state.go:120 +0x18b fp=0x10c0000bcbc0 sp=0x10c0000bcb68 pc=0x62910b
gvisor.dev/gvisor/pkg/state.safely(0x0)
 gvisor.dev/gvisor/pkg/state/state.go:321 +0x71 fp=0x10c0000bcc00 sp=0x10c0000bcbc0 pc=0x629591
gvisor.dev/gvisor/pkg/state.Load({0x6d2760, 0x10c000018180}, {0x6d2320, 0x10c000116000}, {0x6cb960, 0x0})
 gvisor.dev/gvisor/pkg/state/state.go:119 +0x1d1 fp=0x10c0000bcd60 sp=0x10c0000bcc00 pc=0x628ed1
gvisor.dev/gvisor.FuzzStateLoad({0x603000001900, 0x17, 0x17})
 gvisor.dev/gvisor/state_fuzzer.go:28 +0xdf fp=0x10c0000bce08 sp=0x10c0000bcd60 pc=0x62e8bf
main.LLVMFuzzerTestOneInput(...)
 ./main.2517388302.go:21
_cgoexp_e7a74286e976_LLVMFuzzerTestOneInput(0x7ffdc4a48768)
 _cgo_gotypes.go:47 +0x49 fp=0x10c0000bce30 sp=0x10c0000bce08 pc=0x62e969
```

```
runtime.cgocallbackg1(0x62e920, 0x0, 0x0)
 runtime/cgocall.go:306 +0x29a fp=0x10c0000bcf00 sp=0x10c0000bce30 pc=0x56203a
runtime.cgocallbackg(0x0, 0x0, 0x0)
 runtime/cgocall.go:232 +0x109 fp=0x10c0000bcf90 sp=0x10c0000bcf00 pc=0x561d09
runtime.cgocallbackg(0x62e920, 0x7ffdc4a48768, 0x0)
 <autogenerated>:1 +0x31 fp=0x10c0000bcfb8 sp=0x10c0000bcf90 pc=0x5be371
runtime.cgocallback(0x0, 0x0, 0x0)
 runtime/asm_amd64.s:915 +0xb3 fp=0x10c0000bcfe0 sp=0x10c0000bcfb8 pc=0x5bbf33
runtime.goexit()
 runtime/asm_amd64.s:1581 +0x1 fp=0x10c0000bcfe8 sp=0x10c0000bcfe0 pc=0x5bc161
AddressSanitizer:DEADLYSIGNAL
=================================================================
==170959==ERROR: AddressSanitizer: ABRT on unknown address 0x03e800029bcf (pc 0x0000005bda41 bp 0x7ffdc4a48680 sp 0x7ffdc4a48668 T0)
    #0 0x5bda41 in runtime.raise.abi0 runtime/sys_linux_amd64.s:165
    #1 0x5a3d97 in runtime.crash runtime/signal_unix.go:861
    #2 0x590130 in runtime.fatalthrow.func1 runtime/panic.go:1257
    #3 0x5b9f25 in runtime.systemstack.abi0 runtime/asm_amd64.s:383

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: ABRT (/clusterfuzz/run_bot/clusterfuzz/bot/builds/gvisor_libfuzzer_asan/custom/gvisor/state_load_fuzz+0x5bda41)
==170959==ABORTING


+----------------------------------------Release Build Unsymbolized Stacktrace (diff)----------------------------------------+

=================================================================
==170959==ERROR: AddressSanitizer: ABRT on unknown address 0x03e800029bcf (pc 0x0000005bda41 bp 0x7ffdc4a48680 sp 0x7ffdc4a48668 T0)
    #0 0x5bda41  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/gvisor_libfuzzer_asan/custom/gvisor/state_load_fuzz+0x5bda41)
    #1 0x5a3d97  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/gvisor_libfuzzer_asan/custom/gvisor/state_load_fuzz+0x5a3d97)
    #2 0x590130  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/gvisor_libfuzzer_asan/custom/gvisor/state_load_fuzz+0x590130)
    #3 0x5b9f25  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/gvisor_libfuzzer_asan/custom/gvisor/state_load_fuzz+0x5b9f25)
```

--- ORIGINAL STACKTRACE ON **REVISION 1** (78 LINES) ---

```
[Environment] ASAN_OPTIONS=exitcode=77
+----------------------------------------Release Build Stacktrace----------------------------------------+
Command: /clusterfuzz/run_bot/clusterfuzz/bot/builds/gvisor_libfuzzer_asan/custom/gvisor/state_load_fuzz -rss_limit_mb=2560 -timeout=60 -runs=100 /clusterfuzz/run_bot/clusterfuzz/bot/inputs/fuzzer-testcases/crash-b1f49ec073cea3594990465bb6ad5537294f6e3b
Time ran: 0.025870323181152344

INFO: Running with entropic power schedule (0xFF, 100).
INFO: Seed: 4105111772
INFO: 5162 Extra Counters
/clusterfuzz/run_bot/clusterfuzz/bot/builds/gvisor_libfuzzer_asan/custom/gvisor/state_load_fuzz: Running 1 inputs 100 time(s) each.
Running: /clusterfuzz/run_bot/clusterfuzz/bot/inputs/fuzzer-testcases/crash-b1f49ec073cea3594990465bb6ad5537294f6e3b
runtime: out of memory: cannot allocate 118738590367744-byte block (3866624 in use)
fatal error: out of memory

goroutine 17 [running, locked to thread]:
runtime.throw({0x64d1d3, 0x0})
 runtime/panic.go:1198 +0x71 fp=0x10c0000be4d8 sp=0x10c0000be4a8 pc=0x58fe71
runtime.(*mcache).allocLarge(0x7fdffc018008, 0x6bfdfb5fefd0, 0x80, 0x0)
 runtime/mcache.go:229 +0x22e fp=0x10c0000be538 sp=0x10c0000be4d8 pc=0x57364e
runtime.mallocgc(0x6bfdfb5fefd0, 0x6b72e0, 0x1)
 runtime/malloc.go:1082 +0x5c5 fp=0x10c0000be5b8 sp=0x10c0000be538 pc=0x56aa05
runtime.makeslice(0x6d2320, 0x10c00020e000, 0x7fe02891ba68)
 runtime/slice.go:98 +0x52 fp=0x10c0000be5e0 sp=0x10c0000be5b8 pc=0x5a4a72
gvisor.dev/gvisor/pkg/state/wire.loadType({0x6d2320, 0x10c00020e000})
 gvisor.dev/gvisor/pkg/state/wire/wire.go:675 +0x88 fp=0x10c0000be658 sp=0x10c0000be5e0 pc=0x61f9c8
gvisor.dev/gvisor/pkg/state/wire.(*Type).load(...)
 gvisor.dev/gvisor/pkg/state/wire/wire.go:699
gvisor.dev/gvisor/pkg/state/wire.Load({0x6d2320, 0x10c00020e000})
 gvisor.dev/gvisor/pkg/state/wire/wire.go:951 +0x7a9 fp=0x10c0000be778 sp=0x10c0000be658 pc=0x6206a9
gvisor.dev/gvisor/pkg/state.(*decodeState).Load.func2()
 gvisor.dev/gvisor/pkg/state/decode.go:616 +0xbe fp=0x10c0000be838 sp=0x10c0000be778 pc=0x627bbe
gvisor.dev/gvisor/pkg/state.safely(0x6d2320)
 gvisor.dev/gvisor/pkg/state/state.go:321 +0x71 fp=0x10c0000be878 sp=0x10c0000be838 pc=0x629591
gvisor.dev/gvisor/pkg/state.(*decodeState).Load(0x10c000210000, {0x0, 0x0, 0x30})
 gvisor.dev/gvisor/pkg/state/decode.go:609 +0x445 fp=0x10c0000beb68 sp=0x10c0000be878 pc=0x626f25
gvisor.dev/gvisor/pkg/state.Load.func1()
 gvisor.dev/gvisor/pkg/state/state.go:120 +0x18b fp=0x10c0000bebc0 sp=0x10c0000beb68 pc=0x62910b
gvisor.dev/gvisor/pkg/state.safely(0x0)
 gvisor.dev/gvisor/pkg/state/state.go:321 +0x71 fp=0x10c0000bec00 sp=0x10c0000bebc0 pc=0x629591
gvisor.dev/gvisor/pkg/state.Load({0x6d2760, 0x10c00001a180}, {0x6d2320, 0x10c00020e000}, {0x6cb960, 0x0})
 gvisor.dev/gvisor/pkg/state/state.go:119 +0x1d1 fp=0x10c0000bed60 sp=0x10c0000bec00 pc=0x628ed1
gvisor.dev/gvisor.FuzzStateLoad({0x603000001900, 0x17, 0x17})
 gvisor.dev/gvisor/state_fuzzer.go:28 +0xdf fp=0x10c0000bee08 sp=0x10c0000bed60 pc=0x62e8bf
main.LLVMFuzzerTestOneInput(...)
 ./main.2517388302.go:21
_cgoexp_e7a74286e976_LLVMFuzzerTestOneInput(0x7ffd89f90af8)
 _cgo_gotypes.go:47 +0x49 fp=0x10c0000bee30 sp=0x10c0000bee08 pc=0x62e969
runtime.cgocallbackg1(0x62e920, 0x0, 0x0)
 runtime/cgocall.go:306 +0x29a fp=0x10c0000bef00 sp=0x10c0000bee30 pc=0x56203a
runtime.cgocallbackg(0x0, 0x0, 0x0)
 runtime/cgocall.go:232 +0x109 fp=0x10c0000bef90 sp=0x10c0000bef00 pc=0x561d09
runtime.cgocallbackg(0x62e920, 0x7ffd89f90af8, 0x0)
 <autogenerated>:1 +0x31 fp=0x10c0000befb8 sp=0x10c0000bef90 pc=0x5be371
runtime.cgocallback(0x0, 0x0, 0x0)
 runtime/asm_amd64.s:915 +0xb3 fp=0x10c0000befe0 sp=0x10c0000befb8 pc=0x5bbf33
runtime.goexit()
 runtime/asm_amd64.s:1581 +0x1 fp=0x10c0000befe8 sp=0x10c0000befe0 pc=0x5bc161
AddressSanitizer:DEADLYSIGNAL
=================================================================
==83938==ERROR: AddressSanitizer: ABRT on unknown address 0x03e8000147e2 (pc 0x0000005bda41 bp 0x7ffd89f90a10 sp 0x7ffd89f909f8 T0)
SCARINESS: 10 (signal)
    #0 0x5bda41 in runtime.raise.abi0 runtime/sys_linux_amd64.s:165
    #1 0x5a3d97 in runtime.crash runtime/signal_unix.go:861
    #2 0x590130 in runtime.fatalthrow.func1 runtime/panic.go:1257
    #3 0x5b9f25 in runtime.systemstack.abi0 runtime/asm_amd64.s:383

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: ABRT (/clusterfuzz/run_bot/clusterfuzz/bot/builds/gvisor_libfuzzer_asan/custom/gvisor/state_load_fuzz+0x5bda41)
==83938==ABORTING


+----------------------------------------Release Build Unsymbolized Stacktrace (diff)----------------------------------------+

==83938==ERROR: AddressSanitizer: ABRT on unknown address 0x03e8000147e2 (pc 0x0000005bda41 bp 0x7ffd89f90a10 sp 0x7ffd89f909f8 T0)
SCARINESS: 10 (signal)
    #0 0x5bda41  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/gvisor_libfuzzer_asan/custom/gvisor/state_load_fuzz+0x5bda41)
    #1 0x5a3d97  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/gvisor_libfuzzer_asan/custom/gvisor/state_load_fuzz+0x5a3d97)
    #2 0x590130  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/gvisor_libfuzzer_asan/custom/gvisor/state_load_fuzz+0x590130)
    #3 0x5b9f25  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/gvisor_libfuzzer_asan/custom/gvisor/state_load_fuzz+0x5b9f25)
```

TESTCASE ANALYSIS ON OTHER JOBS

No reproducible variants found.

METADATA

[2021-11-18 14:19:05 UTC] comput16-20211115-16:27: Fuzz task : Fuzzer libFuzzer_state_load_fuzz generated testcase crashed in 5 seconds (r1).
[2021-11-18 14:27:18 UTC] comput15-20211115-16:27: Minimize task started.
[2021-11-18 14:27:56 UTC] comput15-20211115-16:27: Minimize task errored out: LibFuzzer minimization failed.
[2021-11-22 03:11:05 UTC] comput4-20211115-16:27: Progression task started.
[2021-11-22 03:11:05 UTC] comput4-20211115-16:27: Progression task finished: still crashes on latest custom build.