**~/envoy\_fuzz\_test\_issue/envoy**$ ./bazel-bin/test/extensions/filters/http/common/fuzz/filter\_fuzz\_test test/extensions/filters/http/common/fuzz/filter\_corpus/clusterfuzz-testcase-minimized-filter\_fuzz\_test-6701612180832256 -l trace

[==========] Running 1 test from 1 test suite.

[----------] Global test environment set-up.

[----------] 1 test from CorpusExamples/FuzzerCorpusTest

[ RUN ] CorpusExamples/FuzzerCorpusTest.RunOneCorpusFile/0

[2023-09-25 19:35:47.279][3021517][info][misc] [test/fuzz/main.cc:47] Corpus file: test/extensions/filters/http/common/fuzz/filter\_corpus/clusterfuzz-testcase-minimized-filter\_fuzz\_test-6701612180832256

[2023-09-25 19:35:47.333][3021517][debug][misc] [test/extensions/filters/http/common/fuzz/filter\_fuzz\_test.cc:76] input Filter configuration: name: "envoy.filters.http.wasm"

typed\_config {

[type.googleapis.com/envoy.extensions.filters.http.wasm.v3.Wasm] {

config {

root\_id: "\_||\_"

vm\_config {

code {

remote {

http\_uri {

uri: "envoy.filters.http.rbac"

cluster: "2"

timeout {

}

}

sha256: "z"

retry\_policy {

retry\_back\_off {

base\_interval {

seconds: 4294967296

}

}

}

}

}

}

}

}

}

[2023-09-25 19:35:47.712][3021517][info][misc] [test/test\_common/test\_random\_generator.cc:20] TestRandomGenerator running with seed 209504760

GMOCK WARNING:

Uninteresting mock function call - taking default action specified at:

test/extensions/filters/http/common/fuzz/uber\_filter.cc:20:

Function call: threadFactory()

Returns: @0x6020000d2430 8-byte object <90-A8 11-08 00-00 00-00>

NOTE: You can safely ignore the above warning unless this call should not happen. Do not suppress it by blindly adding an EXPECT\_CALL() if you don't mean to enforce the call. See https://github.com/google/googletest/blob/master/googlemock/docs/cook\_book.md#knowing-when-to-expect for details.

GMOCK WARNING:

Uninteresting mock function call - taking default action specified at:

test/mocks/api/mocks.cc:19:

Function call: randomGenerator()

Returns: @0x985a1e0 8-byte object <B0-53 EA-07 00-00 00-00>

NOTE: You can safely ignore the above warning unless this call should not happen. Do not suppress it by blindly adding an EXPECT\_CALL() if you don't mean to enforce the call. See https://github.com/google/googletest/blob/master/googlemock/docs/cook\_book.md#knowing-when-to-expect for details.

GMOCK WARNING:

Uninteresting mock function call - taking default action specified at:

test/mocks/api/mocks.cc:17:

Function call: fileSystem()

Returns: @0x98598f0 8-byte object <C0-52 EA-07 00-00 00-00>

NOTE: You can safely ignore the above warning unless this call should not happen. Do not suppress it by blindly adding an EXPECT\_CALL() if you don't mean to enforce the call. See https://github.com/google/googletest/blob/master/googlemock/docs/cook\_book.md#knowing-when-to-expect for details.

GMOCK WARNING:

Uninteresting mock function call - taking default action specified at:

test/mocks/api/mocks.cc:20:

Function call: bootstrap()

Returns: @0x985a298 496-byte object <90-99 13-08 00-00 00-00 00-00 00-00 00-00 00-00 00-00 00-00 00-00 00-00 00-00 00-00 00-00 00-00 00-00 00-00 00-00 00-00 00-00 00-00 00-00 00-00 00-00 00-00 00-00 00-00 00-00 00-00 00-00 00-00 ... 00-00 00-00 00-00 00-00 00-00 00-00 00-00 00-00 00-00 00-00 00-00 00-00 00-00 00-00 00-00 00-00 00-00 00-00 00-00 00-00 00-00 00-00 00-00 00-00 00-00 00-00 00-00 00-00 00-00 00-00 00-00 00-00>

NOTE: You can safely ignore the above warning unless this call should not happen. Do not suppress it by blindly adding an EXPECT\_CALL() if you don't mean to enforce the call. See https://github.com/google/googletest/blob/master/googlemock/docs/cook\_book.md#knowing-when-to-expect for details.

[2023-09-25 19:35:47.847][3021517][info][misc] [test/test\_common/test\_random\_generator.cc:20] TestRandomGenerator running with seed 209504760

[2023-09-25 19:35:47.849][3021517][info][config] [./envoy/registry/registry.h:413] Factory 'envoy.network.dns\_resolver.cares' (type '{"envoy.extensions.network.dns\_resolver.cares.v3.CaresDnsResolverConfig"}') registered for tests

[2023-09-25 19:35:47.850][3021517][info][config] [./envoy/registry/registry.h:456] Removed test factory 'envoy.network.dns\_resolver.cares' (type '{"envoy.extensions.network.dns\_resolver.cares.v3.CaresDnsResolverConfig"}')

[2023-09-25 19:35:47.851][3021517][debug][misc] [test/extensions/filters/http/common/fuzz/filter\_fuzz\_test.cc:88] input Filter configuration: name: "envoy.filters.http.wasm"

typed\_config {

[type.googleapis.com/envoy.extensions.filters.http.wasm.v3.Wasm] {

config {

root\_id: "\_||\_"

vm\_config {

code {

remote {

http\_uri {

uri: "envoy.filters.http.rbac"

cluster: "2"

timeout {

}

}

sha256: "z"

retry\_policy {

retry\_back\_off {

base\_interval {

seconds: 4294967296

}

}

}

}

}

}

}

}

}

[2023-09-25 19:35:47.851][3021517][info][misc] [test/extensions/filters/http/common/fuzz/uber\_filter.cc:69] filter name envoy.filters.http.wasm

yanjun wasm FilterConfig

[2023-09-25 19:35:47.857][3021517][warning][wasm] [source/extensions/common/wasm/wasm.cc:328] Wasm remote code fetch is unstable and may cause a crash

test/mocks/thread\_local/mocks.h:65: Failure

Value of: was\_set\_

Actual: false

Expected: true

Stack trace:

0x427695e: Envoy::ThreadLocal::MockInstance::SlotImpl::get()

0x5763083: Envoy::ThreadLocal::TypedSlot<>::get()

0x5762625: Envoy::Extensions::HttpFilters::Wasm::FilterConfig::createFilter()

0x5762130: std::\_\_1::\_\_function::\_\_func<>::operator()()

0x27d9809: std::\_\_1::\_\_function::\_\_value\_func<>::operator()()

0x27830c9: std::\_\_1::function<>::operator()()

0x27819af: Envoy::Extensions::HttpFilters::UberFilterFuzzer::fuzz()

0x26d36e9: LLVMFuzzerTestOneInput

0x5f3101b: Envoy::(anonymous namespace)::FuzzerCorpusTest\_RunOneCorpusFile\_Test::TestBody()

0x7dcc448: testing::internal::HandleExceptionsInMethodIfSupported<>()

0x7dcc10c: testing::Test::Run()

0x7dce1e1: testing::TestInfo::Run()

... Google Test internal frames ...

**source/extensions/filters/http/wasm/wasm\_filter.h:34:54: runtime error: member call on null pointer of type 'Envoy::Extensions::Common::Wasm::PluginHandleSharedPtrThreadLocal'**

SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior source/extensions/filters/http/wasm/wasm\_filter.h:34:54 in

AddressSanitizer:DEADLYSIGNAL

=================================================================

**==3021517==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000008 (pc 0x00000576319e bp 0x7ffe10db59f0 sp 0x7ffe10db59e0 T0)**

==3021517==The signal is caused by a READ memory access.

==3021517==Hint: address points to the zero page.

**error:** failed to decompress '.debug\_aranges', zlib is not available

**error:** failed to decompress '.debug\_info', zlib is not available

**error:** failed to decompress '.debug\_abbrev', zlib is not available

**error:** failed to decompress '.debug\_line', zlib is not available

**error:** failed to decompress '.debug\_str', zlib is not available

**error:** failed to decompress '.debug\_line\_str', zlib is not available

**error:** failed to decompress '.debug\_loclists', zlib is not available

**error:** failed to decompress '.debug\_rnglists', zlib is not available

#0 0x576319e in std::\_\_1::shared\_ptr<Envoy::Extensions::Common::Wasm::PluginHandle>::shared\_ptr(std::\_\_1::shared\_ptr<Envoy::Extensions::Common::Wasm::PluginHandle> const&) /opt/llvm/bin/../include/c++/v1/\_\_memory/shared\_ptr.h

#1 0x576264d in Envoy::Extensions::HttpFilters::Wasm::FilterConfig::createFilter() /proc/self/cwd/./source/extensions/filters/http/wasm/wasm\_filter.h:34:36

#2 0x576212f in std::\_\_1::\_\_function::\_\_func<Envoy::Extensions::HttpFilters::Wasm::WasmFilterConfig::createFilterFactoryFromProtoTyped(envoy::extensions::filters::http::wasm::v3::Wasm const&, std::\_\_1::basic\_string<char, std::\_\_1::char\_traits<char>, std::\_\_1::allocator<char> > const&, Envoy::Server::Configuration::FactoryContext&)::$\_0, std::\_\_1::allocator<Envoy::Extensions::HttpFilters::Wasm::WasmFilterConfig::createFilterFactoryFromProtoTyped(envoy::extensions::filters::http::wasm::v3::Wasm const&, std::\_\_1::basic\_string<char, std::\_\_1::char\_traits<char>, std::\_\_1::allocator<char> > const&, Envoy::Server::Configuration::FactoryContext&)::$\_0>, void (Envoy::Http::FilterChainFactoryCallbacks&)>::operator()(Envoy::Http::FilterChainFactoryCallbacks&) /proc/self/cwd/source/extensions/filters/http/wasm/config.cc:23:34

#3 0x27d9808 in std::\_\_1::\_\_function::\_\_value\_func<void (Envoy::Http::FilterChainFactoryCallbacks&)>::operator()(Envoy::Http::FilterChainFactoryCallbacks&) const /opt/llvm/bin/../include/c++/v1/\_\_functional/function.h:507:16

#4 0x27830c8 in std::\_\_1::function<void (Envoy::Http::FilterChainFactoryCallbacks&)>::operator()(Envoy::Http::FilterChainFactoryCallbacks&) const /opt/llvm/bin/../include/c++/v1/\_\_functional/function.h:1184:12

#5 0x27819ae in Envoy::Extensions::HttpFilters::UberFilterFuzzer::fuzz(envoy::extensions::filters::network::http\_connection\_manager::v3::HttpFilter const&, test::fuzz::HttpData const&, test::fuzz::HttpData const&) /proc/self/cwd/test/extensions/filters/http/common/fuzz/uber\_filter.cc:77:5

#6 0x26d36e8 in LLVMFuzzerTestOneInput /proc/self/cwd/test/extensions/filters/http/common/fuzz/filter\_fuzz\_test.cc:90:12

#7 0x5f3101a in Envoy::(anonymous namespace)::FuzzerCorpusTest\_RunOneCorpusFile\_Test::TestBody() /proc/self/cwd/test/fuzz/main.cc:50:3

#8 0x7dcc447 in void testing::internal::HandleExceptionsInMethodIfSupported<testing::Test, void>(testing::Test\*, void (testing::Test::\*)(), char const\*) /proc/self/cwd/external/com\_google\_googletest/googletest/src/gtest.cc:2580:10

#9 0x7dcc10b in testing::Test::Run() /proc/self/cwd/external/com\_google\_googletest/googletest/src/gtest.cc:2655:5

#10 0x7dce1e0 in testing::TestInfo::Run() /proc/self/cwd/external/com\_google\_googletest/googletest/src/gtest.cc:2832:11

#11 0x7dd0b5a in testing::TestSuite::Run() /proc/self/cwd/external/com\_google\_googletest/googletest/src/gtest.cc:2986:28

#12 0x7deac0b in testing::internal::UnitTestImpl::RunAllTests() /proc/self/cwd/external/com\_google\_googletest/googletest/src/gtest.cc:5697:44

#13 0x7de9fd7 in bool testing::internal::HandleExceptionsInMethodIfSupported<testing::internal::UnitTestImpl, bool>(testing::internal::UnitTestImpl\*, bool (testing::internal::UnitTestImpl::\*)(), char const\*) /proc/self/cwd/external/com\_google\_googletest/googletest/src/gtest.cc:2580:10

#14 0x7de9b2d in testing::UnitTest::Run() /proc/self/cwd/external/com\_google\_googletest/googletest/src/gtest.cc:5280:10

#15 0x5f2e615 in main /proc/self/cwd/external/com\_google\_googletest/googletest/include/gtest/gtest.h:2485:46

#16 0x7fdd244086c9 (/lib/x86\_64-linux-gnu/libc.so.6+0x276c9) (BuildId: f4017039b18cb668db130b83647b6a0dbefd4414)

#17 0x7fdd24408784 in \_\_libc\_start\_main (/lib/x86\_64-linux-gnu/libc.so.6+0x27784) (BuildId: f4017039b18cb668db130b83647b6a0dbefd4414)

#18 0x261fb2d in \_start (/usr/local/google/home/yanjunxiang/.cache/bazel/\_bazel\_yanjunxiang/c9e0c5a2b4627286a241afa2f7502905/execroot/envoy/bazel-out/k8-opt/bin/test/extensions/filters/http/common/fuzz/filter\_fuzz\_test+0x261fb2d)

AddressSanitizer can not provide additional info.

SUMMARY: AddressSanitizer: SEGV /opt/llvm/bin/../include/c++/v1/\_\_memory/shared\_ptr.h in std::\_\_1::shared\_ptr<Envoy::Extensions::Common::Wasm::PluginHandle>::shared\_ptr(std::\_\_1::shared\_ptr<Envoy::Extensions::Common::Wasm::PluginHandle> const&)

==3021517==ABORTING