

[New issue](#)[Jump to bottom](#)

# CVE-2022-45474: Use-after-free in event\_cb when drachtio-server receives a call #240

✓ Closed asarubbo opened this issue 8 days ago · 2 comments

asarubbo commented 8 days ago

Hello,

this is a follow-up after the private disclosure.

When `drachtio-server` receives a call, if you run it via a debugger (valgrind in this case), you will see a use-after-free that happens by default.

```
valgrind /usr/local/bin/drachtio --contact 'sip:PUBLIC_IP;transport=udp' --contact
'sip:PUBLIC_IP;transport=tcp' --address 0.0.0.0 --port 9022 --homer 127.0.0.1:9060 --homer-id 10

==12406== Memcheck, a memory error detector
==12406== Copyright (C) 2002-2017, and GNU GPL'd, by Julian Seward et al.
==12406== Using Valgrind-3.14.0 and LibVEX; rerun with -h for copyright info
==12406== Command: /usr/local/bin/drachtio --contact sip:PUBLIC_IP;transport=udp --contact
sip:PUBLIC_IP;transport=tcp --address 0.0.0.0 --port 9022 --homer 127.0.0.1:9060 --homer-id 10
==12406==
checking for blacklist in config
did not find blacklist at all
==12406== Warning: invalid file descriptor -1 in syscall close()
==12406== Thread 3:
==12406== Conditional jump or move depends on uninitialised value(s)
==12406==    at 0x4838C65: strlen (in /usr/lib/x86_64-linux-gnu/valgrind/vgpreload_memcheck-amd64-
linux.so)
==12406==    by 0x240146: drachtio::write_cb(void*, unsigned long, unsigned long,
drachtio::RequestHandler::_ConnInfo*) (request-handler.cpp:344)
==12406==    by 0x4870733: ??? (in /usr/lib/x86_64-linux-gnu/libcurl.so.4.5.0)
==12406==    by 0x488348A: ??? (in /usr/lib/x86_64-linux-gnu/libcurl.so.4.5.0)
==12406==    by 0x488CAD2: ??? (in /usr/lib/x86_64-linux-gnu/libcurl.so.4.5.0)
==12406==    by 0x488E15C: ??? (in /usr/lib/x86_64-linux-gnu/libcurl.so.4.5.0)
==12406==    by 0x488E2C4: curl_multi_socket_action (in /usr/lib/x86_64-linux-
gnu/libcurl.so.4.5.0)
==12406==    by 0x2409A6: drachtio::timer_cb(boost::system::error_code const&,
drachtio::RequestHandler::_GlobalInfo*) [clone .part.450] (request-handler.cpp:333)
==12406==    by 0x24119F: timer_cb (error_code.hpp:315)
```

```

==12406== by 0x24119F: drachtio::multi_timer_cb(void*, long,
drachtio::RequestHandler::_GlobalInfo*) (request-handler.cpp:169)
==12406== by 0x488A47B: ??? (in /usr/lib/x86_64-linux-gnu/libcurl.so.4.5.0)
==12406== by 0x488BC0B: curl_multi_add_handle (in /usr/lib/x86_64-linux-gnu/libcurl.so.4.5.0)
==12406== by 0x24294C: drachtio::RequestHandler::startRequest(std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> > const&, std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> > const&, std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> > const&, std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> > const&, bool) (request-handler.cpp:538)
==12406==
==12406== Conditional jump or move depends on uninitialised value(s)
==12406== at 0x4838B06: strncat (in /usr/lib/x86_64-linux-gnu/valgrind/vgpreload_memcheck-
amd64-linux.so)
==12406== by 0x24022D: drachtio::write_cb(void*, unsigned long, unsigned long,
drachtio::RequestHandler::_ConnInfo*) (request-handler.cpp:351)
==12406== by 0x4870733: ??? (in /usr/lib/x86_64-linux-gnu/libcurl.so.4.5.0)
==12406== by 0x488348A: ??? (in /usr/lib/x86_64-linux-gnu/libcurl.so.4.5.0)
==12406== by 0x488CAD2: ??? (in /usr/lib/x86_64-linux-gnu/libcurl.so.4.5.0)
==12406== by 0x488E15C: ??? (in /usr/lib/x86_64-linux-gnu/libcurl.so.4.5.0)
==12406== by 0x488E2C4: curl_multi_socket_action (in /usr/lib/x86_64-linux-
gnu/libcurl.so.4.5.0)
==12406== by 0x2409A6: drachtio::timer_cb(boost::system::error_code const&,
drachtio::RequestHandler::_GlobalInfo*) [clone .part.450] (request-handler.cpp:333)
==12406== by 0x24119F: timer_cb (error_code.hpp:315)
==12406== by 0x24119F: drachtio::multi_timer_cb(void*, long,
drachtio::RequestHandler::_GlobalInfo*) (request-handler.cpp:169)
==12406== by 0x488A47B: ??? (in /usr/lib/x86_64-linux-gnu/libcurl.so.4.5.0)
==12406== by 0x488BC0B: curl_multi_add_handle (in /usr/lib/x86_64-linux-gnu/libcurl.so.4.5.0)
==12406== by 0x24294C: drachtio::RequestHandler::startRequest(std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> > const&, std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> > const&, std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> > const&, std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> > const&, bool) (request-handler.cpp:538)
==12406==
==12406== Invalid read of size 4
==12406== at 0x241585: drachtio::event_cb(drachtio::RequestHandler::_GlobalInfo*, int, int,
boost::system::error_code const&, int*) (request-handler.cpp:280)
==12406== by 0x244C91: operator()<void (*) (drachtio::RequestHandler::_GlobalInfo*, int, int,
const boost::system::error_code&, int*), boost::_bi::rlist2<const boost::system::error_code&,
long unsigned int const&> > (bind.hpp:510)
==12406== by 0x244C91: operator()<const boost::system::error_code&, long unsigned int const&>
(bind.hpp:1297)
==12406== by 0x244C91: operator() (bind_handler.hpp:289)
==12406== by 0x244C91:
asio_handler_invoke<boost::asio::detail::binder2<boost::_bi::bind_t<void, void (*)
(drachtio::RequestHandler::_GlobalInfo*, int, int, const boost::system::error_code&, int*),
boost::_bi::list5<boost::_bi::value<drachtio::RequestHandler::_GlobalInfo*>,
boost::_bi::value<int>, boost::_bi::value<int>, boost::arg<1>, boost::_bi::value<int*> > >,
boost::system::error_code, long unsigned int> > (handler_invoke_hook.hpp:88)
==12406== by 0x244C91: invoke<boost::asio::detail::binder2<boost::_bi::bind_t<void, void (*)
(drachtio::RequestHandler::_GlobalInfo*, int, int, const boost::system::error_code&, int*),
boost::_bi::list5<boost::_bi::value<drachtio::RequestHandler::_GlobalInfo*>,
boost::_bi::value<int>, boost::_bi::value<int>, boost::arg<1>, boost::_bi::value<int*> > >,
boost::system::error_code, long unsigned int>, boost::_bi::bind_t<void, void (*)
(drachtio::RequestHandler::_GlobalInfo*, int, int, const boost::system::error_code&, int*),
boost::_bi::list5<boost::_bi::value<drachtio::RequestHandler::_GlobalInfo*>,

```

```

boost::_bi::value<int>, boost::_bi::value<int>, boost::arg<1>, boost::_bi::value<int*> > > >
(handler_invoke_helpers.hpp:54)
==12406== by 0x244C91: complete<boost::asio::detail::binder2<boost::_bi::bind_t<void, void (*)
(drachtio::RequestHandler::_GlobalInfo*, int, int, const boost::system::error_code&, int*),
boost::_bi::list5<boost::_bi::value<drachtio::RequestHandler::_GlobalInfo*>,
boost::_bi::value<int>, boost::_bi::value<int>, boost::arg<1>, boost::_bi::value<int*> > >,
boost::system::error_code, long unsigned int> > (handler_work.hpp:512)
==12406== by 0x244C91: boost::asio::detail::reactive_null_buffers_op<boost::_bi::bind_t<void,
void (*)>(drachtio::RequestHandler::_GlobalInfo*, int, int, boost::system::error_code const&,
int*), boost::_bi::list5<boost::_bi::value<drachtio::RequestHandler::_GlobalInfo*>,
boost::_bi::value<int>, boost::_bi::value<int>, boost::arg<1>, boost::_bi::value<int*> > >,
boost::asio::any_io_executor>::do_complete(void*, boost::asio::detail::scheduler_operation*,
boost::system::error_code const&, unsigned long) (reactive_null_buffers_op.hpp:84)
==12406== by 0x1C6DB6: complete (scheduler_operation.hpp:40)
==12406== by 0x1C6DB6: do_complete (epoll_reactor.hpp:806)
==12406== by 0x1C6DB6: boost::asio::detail::epoll_reactor::descriptor_state::do_complete(void*,
boost::asio::detail::scheduler_operation*, boost::system::error_code const&, unsigned long)
(epoll_reactor.hpp:796)
==12406== by 0x1C68CB: complete (scheduler_operation.hpp:40)
==12406== by 0x1C68CB: do_run_one (scheduler.hpp:492)
==12406== by 0x1C68CB: boost::asio::detail::scheduler::run(boost::system::error_code&)
(scheduler.hpp:210)
==12406== by 0x240096: run (io_context.hpp:63)
==12406== by 0x240096: drachtio::RequestHandler::threadFunc() (request-handler.cpp:448)
==12406== by 0x4D67B2E: ??? (in /usr/lib/x86_64-linux-gnu/libstdc++.so.6.0.25)
==12406== by 0x48EDFA2: start_thread (pthread_create.c:486)
==12406== by 0x50C606E: clone (clone.S:95)
==12406== Address 0x73bfaa0 is 0 bytes inside a block of size 4 free'd
==12406== at 0x48369AB: free (in /usr/lib/x86_64-linux-gnu/valgrind/vgpreload_memcheck-amd64-
linux.so)
==12406== by 0x24140C: remsock (request-handler.cpp:107)
==12406== by 0x24140C: drachtio::sock_cb(void*, int, int, void*, void*) (request-
handler.cpp:86)
==12406== by 0x488AAC0: ??? (in /usr/lib/x86_64-linux-gnu/libcurl.so.4.5.0)
==12406== by 0x488E179: ??? (in /usr/lib/x86_64-linux-gnu/libcurl.so.4.5.0)
==12406== by 0x488E2C4: curl_multi_socket_action (in /usr/lib/x86_64-linux-
gnu/libcurl.so.4.5.0)
==12406== by 0x2409A6: drachtio::timer_cb(boost::system::error_code const&,
drachtio::RequestHandler::_GlobalInfo*) [clone .part.450] (request-handler.cpp:333)
==12406== by 0x24119F: timer_cb (error_code.hpp:315)
==12406== by 0x24119F: drachtio::multi_timer_cb(void*, long,
drachtio::RequestHandler::_GlobalInfo*) (request-handler.cpp:169)
==12406== by 0x488A47B: ??? (in /usr/lib/x86_64-linux-gnu/libcurl.so.4.5.0)
==12406== by 0x488E2DF: curl_multi_socket_action (in /usr/lib/x86_64-linux-
gnu/libcurl.so.4.5.0)
==12406== by 0x2409A6: drachtio::timer_cb(boost::system::error_code const&,
drachtio::RequestHandler::_GlobalInfo*) [clone .part.450] (request-handler.cpp:333)
==12406== by 0x24119F: timer_cb (error_code.hpp:315)
==12406== by 0x24119F: drachtio::multi_timer_cb(void*, long,
drachtio::RequestHandler::_GlobalInfo*) (request-handler.cpp:169)
==12406== by 0x488A47B: ??? (in /usr/lib/x86_64-linux-gnu/libcurl.so.4.5.0)
==12406== Block was alloc'd at
==12406== at 0x4837B65: calloc (in /usr/lib/x86_64-linux-gnu/valgrind/vgpreload_memcheck-amd64-
linux.so)
==12406== by 0x241423: addsock (request-handler.cpp:100)
==12406== by 0x241423: drachtio::sock_cb(void*, int, int, void*, void*) (request-

```

```

handler.cpp:90)
==12406== by 0x488A9D0: ??? (in /usr/lib/x86_64-linux-gnu/libcurl.so.4.5.0)
==12406== by 0x488E179: ??? (in /usr/lib/x86_64-linux-gnu/libcurl.so.4.5.0)
==12406== by 0x488E2C4: curl_multi_socket_action (in /usr/lib/x86_64-linux-
gnu/libcurl.so.4.5.0)
==12406== by 0x2409A6: drachtio::timer_cb(boost::system::error_code const&,
drachtio::RequestHandler::_GlobalInfo*) [clone .part.450] (request-handler.cpp:333)
==12406== by 0x24119F: timer_cb (error_code.hpp:315)
==12406== by 0x24119F: drachtio::multi_timer_cb(void*, long,
drachtio::RequestHandler::_GlobalInfo*) (request-handler.cpp:169)
==12406== by 0x488A47B: ??? (in /usr/lib/x86_64-linux-gnu/libcurl.so.4.5.0)
==12406== by 0x488BC0B: curl_multi_add_handle (in /usr/lib/x86_64-linux-gnu/libcurl.so.4.5.0)
==12406== by 0x24294C: drachtio::RequestHandler::startRequest(std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> > const&, std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> > const&, std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> > const&, std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> > const&, bool) (request-handler.cpp:538)
==12406== by 0x243665: __invoke_impl<void, void (drachtio::RequestHandler::*&)(const
std::__cxx11::basic_string<char>&, const std::__cxx11::basic_string<char>&, const
std::__cxx11::basic_string<char>&, const std::__cxx11::basic_string<char>&, bool),
drachtio::RequestHandler*&, std::__cxx11::basic_string<char, std::char_traits<char>,
std::allocator<char> >&, std::__cxx11::basic_string<char, std::char_traits<char>,
std::allocator<char> >&, std::__cxx11::basic_string<char, std::char_traits<char>,
std::allocator<char> >&, std::__cxx11::basic_string<char, std::char_traits<char>,
std::allocator<char> >&, std::__cxx11::basic_string<char, std::char_traits<char>,
std::allocator<char> >&, bool&> (invoke.h:73)
==12406== by 0x243665: __invoke<void (drachtio::RequestHandler::*&)(const
std::__cxx11::basic_string<char>&, const std::__cxx11::basic_string<char>&, const
std::__cxx11::basic_string<char>&, const std::__cxx11::basic_string<char>&, bool),
drachtio::RequestHandler*&, std::__cxx11::basic_string<char, std::char_traits<char>,
std::allocator<char> >&, std::__cxx11::basic_string<char, std::char_traits<char>,
std::allocator<char> >&, std::__cxx11::basic_string<char, std::char_traits<char>,
std::allocator<char> >&, std::__cxx11::basic_string<char, std::char_traits<char>,
std::allocator<char> >&, std::__cxx11::basic_string<char, std::char_traits<char>,
std::allocator<char> >&, bool&> (invoke.h:95)
==12406== by 0x243665: __call<void, 0, 1, 2, 3, 4, 5> (functional:400)
==12406== by 0x243665: operator()<> (functional:484)
==12406== by 0x243665: asio_handler_invoke<std::_Bind<void (drachtio::RequestHandler::*
(drachtio::RequestHandler*, std::__cxx11::basic_string<char>, std::__cxx11::basic_string<char>,
std::__cxx11::basic_string<char>, std::__cxx11::basic_string<char>, bool))(const
std::__cxx11::basic_string<char>&, const std::__cxx11::basic_string<char>&, const
std::__cxx11::basic_string<char>&, const std::__cxx11::basic_string<char>&, bool)> >
(handler_invoke_hook.hpp:88)
==12406== by 0x243665: invoke<std::_Bind<void (drachtio::RequestHandler::*
(drachtio::RequestHandler*, std::__cxx11::basic_string<char>, std::__cxx11::basic_string<char>,
std::__cxx11::basic_string<char>, std::__cxx11::basic_string<char>, bool))(const
std::__cxx11::basic_string<char>&, const std::__cxx11::basic_string<char>&, const
std::__cxx11::basic_string<char>&, const std::__cxx11::basic_string<char>&, bool)>,
std::_Bind<void (drachtio::RequestHandler::*(drachtio::RequestHandler*,
std::__cxx11::basic_string<char>, std::__cxx11::basic_string<char>,
std::__cxx11::basic_string<char>, std::__cxx11::basic_string<char>, bool))(const
std::__cxx11::basic_string<char>&, const std::__cxx11::basic_string<char>&, const
std::__cxx11::basic_string<char>&, const std::__cxx11::basic_string<char>&, bool)> >
(handler_invoke_helpers.hpp:54)
==12406== by 0x243665: complete<std::_Bind<void (drachtio::RequestHandler::*
(drachtio::RequestHandler*, std::__cxx11::basic_string<char>, std::__cxx11::basic_string<char>,
std::__cxx11::basic_string<char>, std::__cxx11::basic_string<char>, bool))(const
std::__cxx11::basic_string<char>&, const std::__cxx11::basic_string<char>&, const

```

```

std::__cxx11::basic_string<char>&, const std::__cxx11::basic_string<char>&, bool)> >
(handler_work.hpp:512)
==12406== by 0x243665: boost::asio::detail::completion_handler<std::_Bind<void
(drachtio::RequestHandler::*(drachtio::RequestHandler*, std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> >, std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> >, std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> >, std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> >, bool))>(std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> > const&, std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> > const&, std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> > const&, std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> > const&, bool)>,>
boost::asio::io_context::basic_executor_type<std::allocator<void>, 0ul> >::do_complete(void*,
boost::asio::detail::scheduler_operation*, boost::system::error_code const&, unsigned long)
(completion_handler.hpp:74)
==12406== by 0x1C68CB: complete (scheduler_operation.hpp:40)
==12406== by 0x1C68CB: do_run_one (scheduler.ipp:492)
==12406== by 0x1C68CB: boost::asio::detail::scheduler::run(boost::system::error_code&)
(scheduler.ipp:210)
==12406==
==12406== Invalid read of size 4
==12406== at 0x241651: drachtio::event_cb(drachtio::RequestHandler::_GlobalInfo*, int, int,
boost::system::error_code const&, int*) (request-handler.cpp:297)
==12406== by 0x244C91: operator()<void (*)>(drachtio::RequestHandler::_GlobalInfo*, int, int,
const boost::system::error_code&, int*), boost::_bi::rrlist2<const boost::system::error_code&,
long unsigned int const&> > (bind.hpp:510)
==12406== by 0x244C91: operator()<const boost::system::error_code&, long unsigned int const&>
(bind.hpp:1297)
==12406== by 0x244C91: operator() (bind_handler.hpp:289)
==12406== by 0x244C91:
asio_handler_invoke<boost::asio::detail::binder2<boost::_bi::bind_t<void, void (*)
(drachtio::RequestHandler::_GlobalInfo*, int, int, const boost::system::error_code&, int*),
boost::_bi::list5<boost::_bi::value<drachtio::RequestHandler::_GlobalInfo*>,
boost::_bi::value<int>, boost::_bi::value<int>, boost::arg<1>, boost::_bi::value<int*> > >,
boost::system::error_code, long unsigned int> > (handler_invoke_hook.hpp:88)
==12406== by 0x244C91: invoke<boost::asio::detail::binder2<boost::_bi::bind_t<void, void (*)
(drachtio::RequestHandler::_GlobalInfo*, int, int, const boost::system::error_code&, int*),
boost::_bi::list5<boost::_bi::value<drachtio::RequestHandler::_GlobalInfo*>,
boost::_bi::value<int>, boost::_bi::value<int>, boost::arg<1>, boost::_bi::value<int*> > >,
boost::system::error_code, long unsigned int>, boost::_bi::bind_t<void, void (*)
(drachtio::RequestHandler::_GlobalInfo*, int, int, const boost::system::error_code&, int*),
boost::_bi::list5<boost::_bi::value<drachtio::RequestHandler::_GlobalInfo*>,
boost::_bi::value<int>, boost::_bi::value<int>, boost::arg<1>, boost::_bi::value<int*> > > >
(handler_invoke_helpers.hpp:54)
==12406== by 0x244C91: complete<boost::asio::detail::binder2<boost::_bi::bind_t<void, void (*)
(drachtio::RequestHandler::_GlobalInfo*, int, int, const boost::system::error_code&, int*),
boost::_bi::list5<boost::_bi::value<drachtio::RequestHandler::_GlobalInfo*>,
boost::_bi::value<int>, boost::_bi::value<int>, boost::arg<1>, boost::_bi::value<int*> > >,
boost::system::error_code, long unsigned int> > (handler_work.hpp:512)
==12406== by 0x244C91: boost::asio::detail::reactive_null_buffers_op<boost::_bi::bind_t<void,
void (*)>(drachtio::RequestHandler::_GlobalInfo*, int, int, boost::system::error_code const&,
int*), boost::_bi::list5<boost::_bi::value<drachtio::RequestHandler::_GlobalInfo*>,
boost::_bi::value<int>, boost::_bi::value<int>, boost::arg<1>, boost::_bi::value<int*> > >,
boost::asio::any_io_executor>::do_complete(void*, boost::asio::detail::scheduler_operation*,
boost::system::error_code const&, unsigned long) (reactive_null_buffers_op.hpp:84)
==12406== by 0x1C6DB6: complete (scheduler_operation.hpp:40)

```

```
==12406== by 0x1C6DB6: do_complete (epoll_reactor.ipp:806)
==12406== by 0x1C6DB6: boost::asio::detail::epoll_reactor::descriptor_state::do_complete(void*,
boost::asio::detail::scheduler_operation*, boost::system::error_code const&, unsigned long)
(epoll_reactor.ipp:796)
==12406== by 0x1C68CB: complete (scheduler_operation.hpp:40)
==12406== by 0x1C68CB: do_run_one (scheduler.ipp:492)
==12406== by 0x1C68CB: boost::asio::detail::scheduler::run(boost::system::error_code&)
(scheduler.ipp:210)
==12406== by 0x240096: run (io_context.ipp:63)
==12406== by 0x240096: drachtio::RequestHandler::threadFunc() (request-handler.cpp:448)
==12406== by 0x4D67B2E: ??? (in /usr/lib/x86_64-linux-gnu/libstdc++.so.6.0.25)
==12406== by 0x48EDFA2: start_thread (pthread_create.c:486)
==12406== by 0x50C606E: clone (clone.S:95)
==12406== Address 0x73bf8aa0 is 0 bytes inside a block of size 4 free'd
==12406== at 0x48369AB: free (in /usr/lib/x86_64-linux-gnu/valgrind/vgpreload_memcheck-amd64-
linux.so)
==12406== by 0x24140C: remsock (request-handler.cpp:107)
==12406== by 0x24140C: drachtio::sock_cb(void*, int, int, void*, void*) (request-
handler.cpp:86)
==12406== by 0x488AAC0: ??? (in /usr/lib/x86_64-linux-gnu/libcurl.so.4.5.0)
==12406== by 0x488E179: ??? (in /usr/lib/x86_64-linux-gnu/libcurl.so.4.5.0)
==12406== by 0x488E2C4: curl_multi_socket_action (in /usr/lib/x86_64-linux-
gnu/libcurl.so.4.5.0)
==12406== by 0x2409A6: drachtio::timer_cb(boost::system::error_code const&,
drachtio::RequestHandler::_GlobalInfo*) [clone .part.450] (request-handler.cpp:333)
==12406== by 0x24119F: timer_cb (error_code.hpp:315)
==12406== by 0x24119F: drachtio::multi_timer_cb(void*, long,
drachtio::RequestHandler::_GlobalInfo*) (request-handler.cpp:169)
==12406== by 0x488A47B: ??? (in /usr/lib/x86_64-linux-gnu/libcurl.so.4.5.0)
==12406== by 0x488E2DF: curl_multi_socket_action (in /usr/lib/x86_64-linux-
gnu/libcurl.so.4.5.0)
==12406== by 0x2409A6: drachtio::timer_cb(boost::system::error_code const&,
drachtio::RequestHandler::_GlobalInfo*) [clone .part.450] (request-handler.cpp:333)
==12406== by 0x24119F: timer_cb (error_code.hpp:315)
==12406== by 0x24119F: drachtio::multi_timer_cb(void*, long,
drachtio::RequestHandler::_GlobalInfo*) (request-handler.cpp:169)
==12406== by 0x488A47B: ??? (in /usr/lib/x86_64-linux-gnu/libcurl.so.4.5.0)
==12406== Block was alloc'd at
==12406== at 0x4837B65: calloc (in /usr/lib/x86_64-linux-gnu/valgrind/vgpreload_memcheck-amd64-
linux.so)
==12406== by 0x241423: addsock (request-handler.cpp:100)
==12406== by 0x241423: drachtio::sock_cb(void*, int, int, void*, void*) (request-
handler.cpp:90)
==12406== by 0x488A9D0: ??? (in /usr/lib/x86_64-linux-gnu/libcurl.so.4.5.0)
==12406== by 0x488E179: ??? (in /usr/lib/x86_64-linux-gnu/libcurl.so.4.5.0)
==12406== by 0x488E2C4: curl_multi_socket_action (in /usr/lib/x86_64-linux-
gnu/libcurl.so.4.5.0)
==12406== by 0x2409A6: drachtio::timer_cb(boost::system::error_code const&,
drachtio::RequestHandler::_GlobalInfo*) [clone .part.450] (request-handler.cpp:333)
==12406== by 0x24119F: timer_cb (error_code.hpp:315)
==12406== by 0x24119F: drachtio::multi_timer_cb(void*, long,
drachtio::RequestHandler::_GlobalInfo*) (request-handler.cpp:169)
==12406== by 0x488A47B: ??? (in /usr/lib/x86_64-linux-gnu/libcurl.so.4.5.0)
==12406== by 0x488BC0B: curl_multi_add_handle (in /usr/lib/x86_64-linux-gnu/libcurl.so.4.5.0)
==12406== by 0x24294C: drachtio::RequestHandler::startRequest(std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> > const&, std::__cxx11::basic_string<char,
```




```

std::char_traits<char>, std::allocator<char> > const&, std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> > const&, std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> > const&, bool) (request-handler.cpp:538)
==12406== by 0x243665: __invoke_impl<void, void (drachtio::RequestHandler::*&)(const
std::__cxx11::basic_string<char>&, const std::__cxx11::basic_string<char>&, const
std::__cxx11::basic_string<char>&, const std::__cxx11::basic_string<char>&, bool),
drachtio::RequestHandler*&, std::__cxx11::basic_string<char, std::char_traits<char>,
std::allocator<char> >&, std::__cxx11::basic_string<char, std::char_traits<char>,
std::allocator<char> >&, std::__cxx11::basic_string<char, std::char_traits<char>,
std::allocator<char> >&, std::__cxx11::basic_string<char, std::char_traits<char>,
std::allocator<char> >&, bool&> (invoke.h:73)
==12406== by 0x243665: __invoke<void (drachtio::RequestHandler::*&)(const
std::__cxx11::basic_string<char>&, const std::__cxx11::basic_string<char>&, const
std::__cxx11::basic_string<char>&, const std::__cxx11::basic_string<char>&, bool),
drachtio::RequestHandler*&, std::__cxx11::basic_string<char, std::char_traits<char>,
std::allocator<char> >&, std::__cxx11::basic_string<char, std::char_traits<char>,
std::allocator<char> >&, std::__cxx11::basic_string<char, std::char_traits<char>,
std::allocator<char> >&, std::__cxx11::basic_string<char, std::char_traits<char>,
std::allocator<char> >&, bool&> (invoke.h:95)
==12406== by 0x243665: __call<void, 0, 1, 2, 3, 4, 5> (functional:400)
==12406== by 0x243665: operator()<> (functional:484)
==12406== by 0x243665: asio_handler_invoke<std::_Bind<void (drachtio::RequestHandler::*
(drachtio::RequestHandler*, std::__cxx11::basic_string<char>, std::__cxx11::basic_string<char>,
std::__cxx11::basic_string<char>, std::__cxx11::basic_string<char>, bool))(const
std::__cxx11::basic_string<char>&, const std::__cxx11::basic_string<char>&, const
std::__cxx11::basic_string<char>&, const std::__cxx11::basic_string<char>&, bool)> >
(handler_invoke_hook.hpp:88)
==12406== by 0x243665: invoke<std::_Bind<void (drachtio::RequestHandler::*
(drachtio::RequestHandler*, std::__cxx11::basic_string<char>, std::__cxx11::basic_string<char>,
std::__cxx11::basic_string<char>, std::__cxx11::basic_string<char>, bool))(const
std::__cxx11::basic_string<char>&, const std::__cxx11::basic_string<char>&, const
std::__cxx11::basic_string<char>&, const std::__cxx11::basic_string<char>&, bool)>,
std::_Bind<void (drachtio::RequestHandler::* (drachtio::RequestHandler*,
std::__cxx11::basic_string<char>, std::__cxx11::basic_string<char>,
std::__cxx11::basic_string<char>, std::__cxx11::basic_string<char>, bool))(const
std::__cxx11::basic_string<char>&, const std::__cxx11::basic_string<char>&, const
std::__cxx11::basic_string<char>&, const std::__cxx11::basic_string<char>&, bool)> >
(handler_invoke_helpers.hpp:54)
==12406== by 0x243665: complete<std::_Bind<void (drachtio::RequestHandler::*
(drachtio::RequestHandler*, std::__cxx11::basic_string<char>, std::__cxx11::basic_string<char>,
std::__cxx11::basic_string<char>, std::__cxx11::basic_string<char>, bool))(const
std::__cxx11::basic_string<char>&, const std::__cxx11::basic_string<char>&, const
std::__cxx11::basic_string<char>&, const std::__cxx11::basic_string<char>&, bool)> >
(handler_work.hpp:512)
==12406== by 0x243665: boost::asio::detail::completion_handler<std::_Bind<void
(drachtio::RequestHandler::* (drachtio::RequestHandler*, std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> >, std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> >, std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> >, std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> >, bool))(std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> > const&, std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> > const&, std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> > const&, std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> > const&, bool)>,
boost::asio::io_context::basic_executor_type<std::allocator<void>, 0ul> >::do_complete(void*,
boost::asio::detail::scheduler_operation*, boost::system::error_code const&, unsigned long)


```

```
(completion_handler.hpp:74)
==12406==    by 0x1C68CB: complete (scheduler_operation.hpp:40)
==12406==    by 0x1C68CB: do_run_one (scheduler.hpp:492)
==12406==    by 0x1C68CB: boost::asio::detail::scheduler::run(boost::system::error_code&)
(scheduler.hpp:210)
==12406==
```

 **davehorton** added a commit that referenced this issue 3 days ago

 **davehorton** fix for use-after-free ([#240](#))



✗ 860f025

 **davehorton** closed this as completed 3 days ago

**davehorton** commented 2 days ago

Collaborator

fixed in v0.8.19-rc12

  **asarubbo** changed the title ~~Use-after-free in event\_cb when drachtio-server receives a call~~ CVE-2022-45474: Use-after-free in event\_cb when drachtio-server receives a call 19 hours ago

**asarubbo** commented 19 hours ago

Author

[CVE-2022-45474](#) has been assigned to this issue

#### Assignees

No one assigned

#### Labels

None yet

#### Projects

None yet

#### Milestone

No milestone

#### Development



Development

No branches or pull requests

---

2 participants

