Agent crashes when receiving invalid Boolean values (not 0 or 1) #389

Closed

j4kb4dw0lf opened on Apr 28, 2025 · edited by j4kb4dw0lf Edits

- Hardware description: x86_64 PC, standard desktop
- OS: Ubuntu 22.04 LTS
- Installation type: Built from source, CMake default flags, FastDDS 2.14
- Version or commit hash: 3.0.1 (main branch)

Steps to reproduce the issue

Send a packet that includes a boolean field with a value different from 0 or 1 (e.g., 2, 255).
You can easily modify a client to do this manually or fuzz the connection.

Expected behavior

The agent should either:

- Normalize the boolean value (e.g., treat anything nonzero as `true`), **or**
- Gracefully reject the packet and log an error.

Actual behavior

The agent crashes immediately when trying to deserialize a boolean field that has an invalid value (neither 0 nor 1). Exceptions are thrown by the FastCDR implementation of the deserializiation but are not caught, leading to undefined behavior and potential security risks (DoS by packet manipulation).

Additional information

This crash affects stability and opens the agent to simple denial-of-service attacks via malformed packets. A check for valid boolean values during deserialization would solve the problem, same would apply if the exception is gracefully caught.

j4kb4dw0lf mentioned this on May 8, 2025

MTU length not validated: possible call to alloc() or realloc()... with size 0 #390

4ntn on May 12, 2025

Hello @**j4kb4dw0lf** ,

I am not being able to reproduce this issue.

Can you point me to somewhere in the code where you think this is happening? Or maybe specify how you are testing this.

On the other issue it was very helpful.

Thanks!

j4kb4dw0lf on May 12, 2025 · edited by j4kb4dw0lf Edits Author

Hello @**4ntn**, in this casae the issue is very easily reproducible using the CREATE_CLIENT submessage which contains a boolean field: `m_properties_flag` that is deserialized here:

Micro-XRCE-DDS-Agent/src/cpp/types/XRCETypes.cpp
Line 1130 in `155cfaa`

```
1130      bool m_properties_flag;
```

if this value is found to be not 0 or 1, as by fastcdr policy:
https://github.com/eProsima/Fast-CDR/blob/36c28c4e5f638c1436c5e709d00ba9b68d358372/src/cpp/FastCdr.cpp#L380
it generates an exception which uncaught crashes the agent. In general the exception is uncaught everytime the deserialization happens for booleans inside the repository and many other kinds of submessages lead to the same issue if they contain "optional" fields in the submessage payload.

4ntn mentioned this on May 13, 2025

Catch CDR exceptions #393

4ntn on May 13, 2025

Hi @**j4kb4dw0lf** , thank you for the guidance.

I have implemented this fix: #393

I will close this issue when the PR is merged.

4ntn closed this as completed on May 13, 2025

Metadata

Assignees

No one assigned

Labels

No labels

Type

No type

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

No branches or pull requests

Participants