ROS 2 Navigation 2组件数值鲁棒性与序列化漏洞报告

漏洞1：AMCL数值鲁棒性漏洞

漏洞类型：数值鲁棒性缺陷
影响组件：ROS 2 Navigation 2中的AMCL（自适应蒙特卡洛定位）包

漏洞描述

AMCL节点在处理包含极端数值的`/amcl_pose`输入消息时，缺乏足够的输入验证和数值边界检查，导致内部粒子滤波器产生数值计算错误。这些错误会传播到粒子云状态中，使得输出的`/particlecloud`消息包含NaN（非数字）或INF（无穷大）值，从而导致定位系统完全失效。

触发条件

向AMCL节点发布包含以下特征的`/amcl_pose`消息：

1. **极端位置值**：

```
pose.pose.position.x = -1.0786174898657036e+252  // 极大负值
pose.pose.position.y = 0.0
pose.pose.position.z = 0.0
```

2. **无效协方差矩阵**：

```
pose.covariance[0] = -INF  // x方差的无穷大负值
pose.covariance[7] = -INF  // y方差的无穷大负值
```

影响表现

1. **直接输出：** `/particlecloud` 话题中的粒子包含NaN/INF值

   ```
   particlecloud.poses[3].position.y = nan  // 或 inf
   ```

2. **系统影响：**
   - 后续导航决策基于错误位置
   - 可能导致机器人行为异常或碰撞

攻击路径分析

```
攻击向量：恶意/amcl_pose消息
    ↓
AMCL缺乏输入验证
    ↓
极端值进入粒子滤波器计算
    ↓
数值计算溢出/除零错误
    ↓
NaN/INF在粒子状态中传播
    ↓
定位输出污染 → 导航系统失效
```

修复建议

建议修复方案：添加输入验证层

- 实现数值范围检查，拒绝超出合理范围的输入
- 验证协方差矩阵的正定性
- 添加异常处理机制，防止数值错误传播

漏洞2：ROSIDL Float32非规范化数值处理漏洞

漏洞类型：数值处理缺陷
影响组件：ROSIDL类型系统序列化模块

漏洞描述

ROSIDL类型系统在序列化denormalized float32（非规范化单精度浮点数）值时，未正确处理指数位为0但尾数位非零的特殊情况，导致序列化过程失败。

触发条件

精确触发值： `1.5294078387616778e-19`
数据类型：denormalized float32（非规范化单精度浮点数）
十六进制表示： `0x848f3420`
二进制模式： `00100000001101001000111110000100`

技术特征

- **指数位：** `00000000`（全零，表示denormalized number）
- **尾数位：** `00000001101001000111110000100`（非零）
- **数值范围：**在float32可表示的最小正规范化数（1.175494e-38）之下
- **序列化特征：**pickle协议4，包含OrderedDict结构，键名为"data"

影响表现

发送包含该精确值的Float32类型消息时，`/idltest_Float32_out`话题完全丢失，消息无法传输。

可能原因

ROSIDL类型系统在序列化denormalized float32值时，未正确处理指数位为0但尾数位非零的特殊情况，导致序列化过程失败。

漏洞3：ROSIDL Int8固定数组边界验证绕过漏洞

漏洞类型：边界验证缺陷
影响组件：ROSIDL类型系统数组验证模块

漏洞描述

Int8固定数组的长度验证逻辑存在缺陷，允许长度完全不匹配的数组通过初步验证，但在后续处理中导致系统失败。

触发条件

数组长度：64个元素
期望长度：4个元素（固定长度数组）

技术特征

- **预期行为**：应该拒绝长度不为4的数组
- **实际行为**：接受了长度为64的数组，但后续处理失败
- **失败点**：序列化过程在验证后阶段失败，话题丢失

影响表现

发送长度不匹配的Int8FixedArray消息时，`/idltest_Int8FixedArray_out`话题丢失，但长度验证未正确拦截非法输入。

漏洞4：ROSIDL序列化往返一致性漏洞

漏洞类型：序列化一致性缺陷
影响组件：ROSIDL类型系统序列化模块

漏洞描述

特定规范化float32值在序列化过程中发生不可逆变化，破坏数据完整性。

触发条件

精确触发值：`2747081.0730923223`
数据类型：规范化float32

十六进制表示： `0x4a2799a1`
二进制模式： 规范化浮点数，指数位非零

特征

1. **输入值：** `2747081.0730923223`
2. **预期行为：** 序列化后再反序列化应得到相同值
3. **实际行为：** 往返序列化后值发生变化
4. **差异类型：** 浮点数二进制表示在序列化过程中发生不可逆变化

影响表现

发送该特定float32值进行往返序列化测试时，输入输出消息不匹配，数据完整性被破坏。
