

Contracts vulnerabilities

Vulnerabilities list: #1

Contracts vulnerabilities	1
Vulnerabilities list: #1	1
Involved contracts and level of the bugs	1
Vulnerabilities	1
1. tokenURI function	1

Involved contracts and level of the bugs

The present document aims to point out some vulnerabilities in the [autonolas-registry](#) contracts.

Vulnerabilities

1. tokenURI function

Severity: Low

The following function is implemented in the GenericRegistry contract:

```
function tokenURI(uint256 unitId) public view virtual override
returns (string memory)
```

This function is defined by the [EIP-721 standard](#). The standard states that the function is supposed to throw if **unitId** is not a valid NFT. However, in our contract, the function does not revert if the **unitId** is out of bounds, but just returns the value of a string with the defined prefix and 64 zeros derived from a zero bytes32 value.

Therefore, we recommend checking the return value of this view function, and if the last 64 symbols are zero, consider it to be an invalid NFT. Also one might use the **exists()** function to preliminary check if the requested NFT Id exists.