


High severity issues

- **Initial Token Distribution / Centralization**

In the constructor function, the deployer is minting tokens for his wallet address. All the initial supply are sent to the contract deployer when deploying the contract. This could be a centralization risk, the deployer can distribute those tokens without obtaining the consensus of the community.



```
1  contract UlelaToken is ERC20 {
2      constructor(
3          string memory name_,
4          string memory symbol_,
5          uint256 amount_
6      ) ERC20(name_, symbol_) {
7          /// *****
8          /// THIS IS Centralization RISK. DEPLOYER IS MINTING TOKEN FOR HIMSELF
9          /// *****
10
11         _mint(_msgSender(), amount_ * (10**uint256(decimals())));
12     }
13 }
14
```

- ✓ **Recommendation**

We recommend the team to be transparent regarding the initial token distribution process, and the team shall make enough efforts to restrict the access of the private key, We also advise the client to adopt Multisig, Timelock, and/or DAO in the project to manage the specific account in this case.