Vitalik Security Audit

Altfolio

Code Review + Launch Stimulation

Thursday, 18 August 2022

Website: www.altfolioapp.io

Twitter: @altfolioapp_io

Telegram: @Altfolioapp

Severity Criteria

Vitalik assesses severity of disclosed vulnerabilities according to a methodology based on OWASP standards.

Vulnerabilities are divided into 3 primary risk categories:

- Low
- Medium
- High

High-level considerations for vulnerabilities span the following key areas when conducting

assessments:

- Malicious Input Handling
- Escalation of privileges
- Arithmetic
- Gas use

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

Details

Name : Altfolio

Symbol: ALT

Total Supply: 50 000 000

Contract Address:

0x121BCf841e987CBC41541496100Fd5741C75C1c9

Contract SHA256 Hash:

0a26aa1282e5d610f80abf21538ed95587eb1dbf090b1b4b45a1b03169b57a2c

Quick Overview & Findings

A simple & totally safe ERC20 token with no taxes, no reflections, & no complex functions.

There is no issue in contract because only standard and verified library & classes are used & compiler version is also up to date.

Its clear that contract has no issues, however to be totally and fully sure we tested Buying and Selling on our local blockchain (which is only used for testing and development and no real funds are used), there was no issue with buying, selling or transferring tokens

Findings:

- Low : 0
- Medium : 0
- High : 0
- Suggest : 0

Testing on local blockchain

First we added liquidity (ALT/WBNB) and then we used 10 testing accounts to buy and then sell $ALT, as you can see in below pictures there is no tax for buying or selling, no tokens get collected inside contract and used gas is also very low.
This testings are done using hardhat and Pancakeswap sdk(npm)

```
roholah@roholah-X541UJ:~/Desktop/audit/hardhat-security-fcc$ yarn sl
yarn run v1.22.15
warning ../../../package.json: No license field
$ hh run utils/mass_buying/sell.js --network localhost
[ '0xf2AB1abFdB630e88c46197473EF260C9f9E016Af' ]
Account Balance 4502480136519450
🟠Action : Sell
50000000000
 🔸Seller : 0xf39Fd6e51aad88F6F4ce6aB8827279cffFb92266
 🔸Sell Amount : 50000000000
 🔸Sell Tax : 0 %
 🔸Gas Used : 118459
 🔸Block Number : 21
 🔸Monitoring Wallets:
Contract : 0 Altfolio
================================
Account Balance 2455617181889
🟠Action : Sell
50000000000
 🔸Seller : 0x70997970C51812dc3A010C7d01b50e0d17dc79C8
 🔸Sell Amount : 50000000000
 🔸Sell Tax : 0 %
 🔸Gas Used : 118459
 🔸Block Number : 23
 🔸Monitoring Wallets:
Contract : 0 Altfolio
================================
Account Balance 2431459842065
🟠Action : Sell
50000000000
 🔸Seller : 0x3C44CdDdB6a900fa2b585dd299e03d12FA4293BC
 🔸Sell Amount : 50000000000
 🔸Sell Tax : 0 %
 🔸Gas Used : 118447
 🔸Block Number : 25
 🔸Monitoring Wallets:
```

selling

```
roholah@roholah-X541UJ:~/Desktop/audit/hardhat-security-fcc$ yarn mb
yarn run v1.22.15
warning ../../../package.json: No license field
$ hh run utils/mass_buying/run.js --network localhost
🟢Action : Buy
 🔸Buyer : 0xf39Fd6e51aad88F6F4ce6aB8827279cffFb92266
 🔸Purchace Amount : 2480136519450
 🔸Buy Tax : 0 %
 🔸Gas Used : 136925
 🔸Monitored Wallets :
Contract : 0 Altfolio
================================
🟢Action : Buy
 🔸Buyer : 0x70997970C51812dc3A010C7d01b50e0d17dc79C8
 🔸Purchace Amount : 2455617181889
 🔸Buy Tax : 0 %
 🔸Gas Used : 119825
 🔸Monitored Wallets :
Contract : 0 Altfolio
================================
🟢Action : Buy
 🔸Buyer : 0x3C44CdDdB6a900fa2b585dd299e03d12FA4293BC
 🔸Purchace Amount : 2431459842065
 🔸Buy Tax : 0 %
 🔸Gas Used : 119813
 🔸Monitored Wallets :
Contract : 0 Altfolio
================================
🟢Action : Buy
 🔸Buyer : 0x90F79bf6EB2c4f870365E785982E1f101E93b906
 🔸Purchace Amount : 2407657407203
 🔸Buy Tax : 0 %
 🔸Gas Used : 119825
 🔸Monitored Wallets :
Contract : 0 Altfolio
================================
```

Buying

Disclaimer

This report is not, nor should be considered, an “endorsement” or “disapproval” of any particular project or team.

This report is not, nor should be considered, an indication of the economics or value of any “product” or “asset” created by any team or project that contracts VITALIK to perform a security assessment.

This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors,business, business model or legal compliance.

This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides investment advice, nor should be leveraged as Investment advice of any sort.

This report represents an extensive assessing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic token sand blockchain technology.

About Vitalik Audit

we are a small yet strong auditing team, we love to read and test smart contracts, if you think you are able to audit a smart contract or you want your project to be audited reach us through one of this ways.

Telegram: t.me/VitalikAudit
Website: https://vitalik-platform.xyz
Owner: t.me/AnanCoder