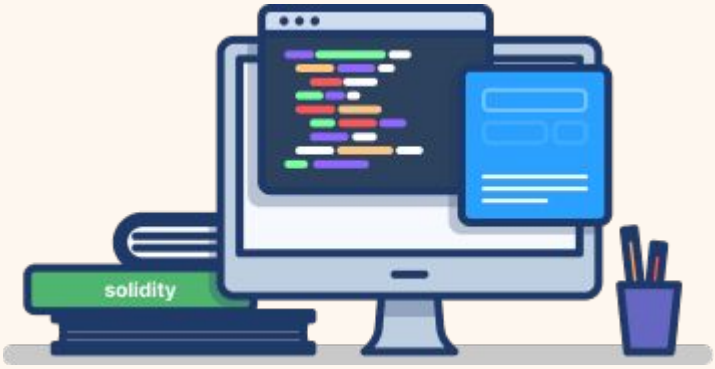
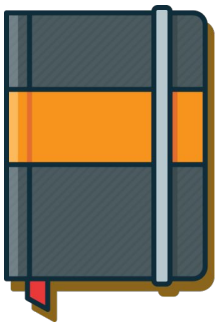
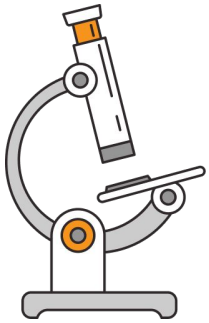
Coinbae Audit

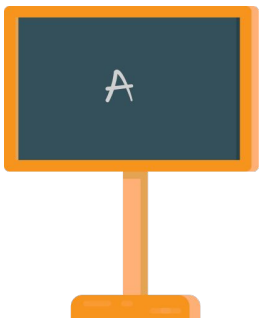


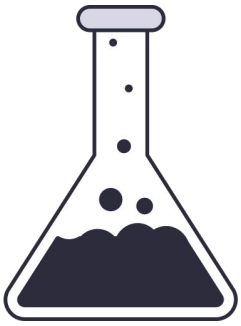
DEAStaking from Deus Finance December 2020

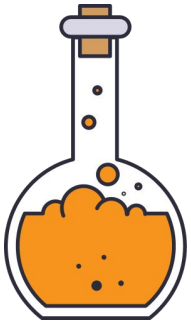
Contents











Introduction

Audit:

In December 2020 Coinbae's audit report division performed an audit for the Deus Finance team (DEAStaking pool).

https://etherscan.io/address/0x1D17d697cAAffE53bf3bFdE761c90D61F6ebdc41#code

Deus Finance:

DEUS lets you trade real-world assets and derivatives, like stocks and commodities, directly on the Ethereum blockchain.

As described in the Deus Finance litepaper.

DEUS finance is a Decentralized Finance (DeFi) protocol that allows bringing any verifiable digital and non-digital asset onto the blockchain. It boosts the transfer of value across many different markets and exchanges with unprecedented ease, transparency, and security. The launch system is currently being built on the Ethereum-blockchain and will be chain-agnostic in the future. It started out originally as development on a tool to manage the asset basket for a community crypto investment pool. This turned into the vision of DEUS as a DAO-governed, decentralized platform that holds and mirrors assets.

More information can be found at https://deus.finance/home/.

Introduction

Overview:

Information:
Ticker: DEA
Type: Token (0x80ab141f324c3d6f2b18b030f1c4e95d4d658778)
Ticker: DEUS
Type: Token (0x3b62f3820e0b035cc4ad602dece6d796bc325325)

Pool, Asset or Contract address:
0x1D17d697cAAffE53bf3bFdE761c90D61F6ebdc41

Supply:
Current: 2,384,600

Explorers:
Etherscan.io

Websites:
https://deus.finance/home/

Links:
Github

Introduction

Compiler related issues:

It is best practice to use the latest version of the solidity compiler supported by the toolset you use. This so it includes all the latest bug fixes of the solidity compiler. When you use for instance the openzeppelin contracts in your code the solidity version you should use should be 0.8.0 because this is the latest version supported.

Caution:

The solidity versions used for the audited contracts are 0.6.11 this version has the following known bugs so the compiled contract might be susceptible to:

EmptyByteArrayCopy – Medium risk

Copying an empty byte array (or string) from memory or calldata to storage can result in data corruption if the target array's length is increased subsequently without storing new data.
https://etherscan.io/solcbuginfo?a=EmptyByteArrayCopy

DynamicArrayCleanup – Medium risk

When assigning a dynamically-sized array with types of size at most 16 bytes in storage causing the assigned array to shrink, some parts of deleted slots were not zeroed out.
https://etherscan.io/solcbuginfo?a=DynamicArrayCleanup

Advice:

Update the contracts to the latest supported version of solidity.

https://etherscan.io/address/0x1D17d697cAAffE53bf3bFdE761c90D61F6ebdc41#code
DEA Staking

Audit Report Scope

Assertions and Property Checking:

1. Solidity assert violation.
2. Solidity AssertionFailed event.

ERC Standards:

1. Incorrect ERC20 implementation.

Solidity Coding Best Practices:

1. Outdated compiler version.
2. No or floating compiler version set.
3. Use of right-to-left-override control character.
4. Shadowing of built-in symbol.
5. Incorrect constructor name.
6. State variable shadows another state variable.
7. Local variable shadows a state variable.
8. Function parameter shadows a state variable.
9. Named return value shadows a state variable.
10. Unary operation without effect Solidity code analysis.
11. Unary operation directly after assignment.
12. Unused state variable.
13. Unused local variable.
14. Function visibility is not set.
15. State variable visibility is not set.
16. Use of deprecated functions: call code(), sha3(), ...
17. Use of deprecated global variables (msg.gas, ...).
18. Use of deprecated keywords (throw, var).
19. Incorrect function state mutability.
20. Does the code conform to the Solidity styleguide.

Convert code to conform Solidity styleguide:

1. Convert all code so that it is structured accordingly the Solidity styleguide.

Audit Report Scope

Categories:

High Severity:

High severity issues opens the contract up for exploitation from malicious actors. We do not recommend deploying contracts with high severity issues.

Medium Severity Issues:

Medium severity issues are errors found in contracts that hampers the effectiveness of the contract and may cause outcomes when interacting with the contract. It is still recommended to fix these issues.

Low Severity Issues:

Low severity issues are warning of minor impact on the overall integrity of the contract. These can be fixed with less urgency.

Audit Report

11	11	0
Identified	Confirmed	Critical

0	8	3
High	Medium	Low

Analysis:
https://etherscan.io/address/0x1D17d697cAAffE53bf3bFdE761c90D61F6ebdc41#code

Risk:
Low (Explained)

Coding best practices:

Function could be marked as external SWC-000:

Calling each function, we can see that the public function uses 496 gas, while the external function uses only 261. The difference is because in public functions, Solidity immediately copies array arguments to memory, while external functions can read directly from calldata. Memory allocation is expensive, whereas reading from calldata is cheap. So if you can, use external instead of public.

Affected lines:

1. function setWallets(address _daoWallet, address _earlyFoundersWallet) public onlyOwner { [#65]
2. function setShares(uint256 _daoShare, uint256 _earlyFoundersShare) public onlyOwner { [#70]
3. function setRewardPerBlock(uint256 _rewardPerBlock) public onlyOwner { [#76]
4. function deposit(uint256 amount) public { [#105]
5. function withdraw(uint256 amount) public { [#123]
6. function emergencyWithdraw() public { [#156]
7. function withdrawAllRewardTokens(address to) public onlyOwner { [#171]
8. function withdrawAllStakedtokens(address to) public onlyOwner { [#178]

High severity issues, Overpowered user:

See the update and teams response on page 10.

Description:

Functions on DEAStaking.sol (setShares, setRewardPerBlock`,setWallets) are callable only from one address if the private key of this address becomes compromised rewards can be changed and this may lead to undesirable consequences.

Line 65:

functionsetWallets(address_daoWallet,address_earlyFoundersWallet)publiconlyOwner{daoWallet=_daoWallet;earlyFoundersWallet=_earlyFoundersWallet;}

Line 70:

functionsetShares(uint256_daoShare,uint256_earlyFoundersShare)publiconlyOwner{withdrawParticleCollector();daoShare=_daoShare;earlyFoundersShare=_earlyFoundersShare;}

Line 70:

functionsetRewardPerBlock(uint256_rewardPerBlock)publiconlyOwner{update();emitRewardPerBlockChanged(rewardPerBlock,_rewardPerBlock);rewardPerBlock=_rewardPerBlock;}

Recommendation:

Use a multisig wallet for overpowered users.

Solved issues (Risk moved to Low):

Update:

After pointing out the high severity issues to the Deus Finance team consensus was reached and corroborated by the Coinbae team. The Deus Finance team did in fact place control of the contracts under ownership of the DAO(Decentralized autonomous organization) as can be seen in this tx id.

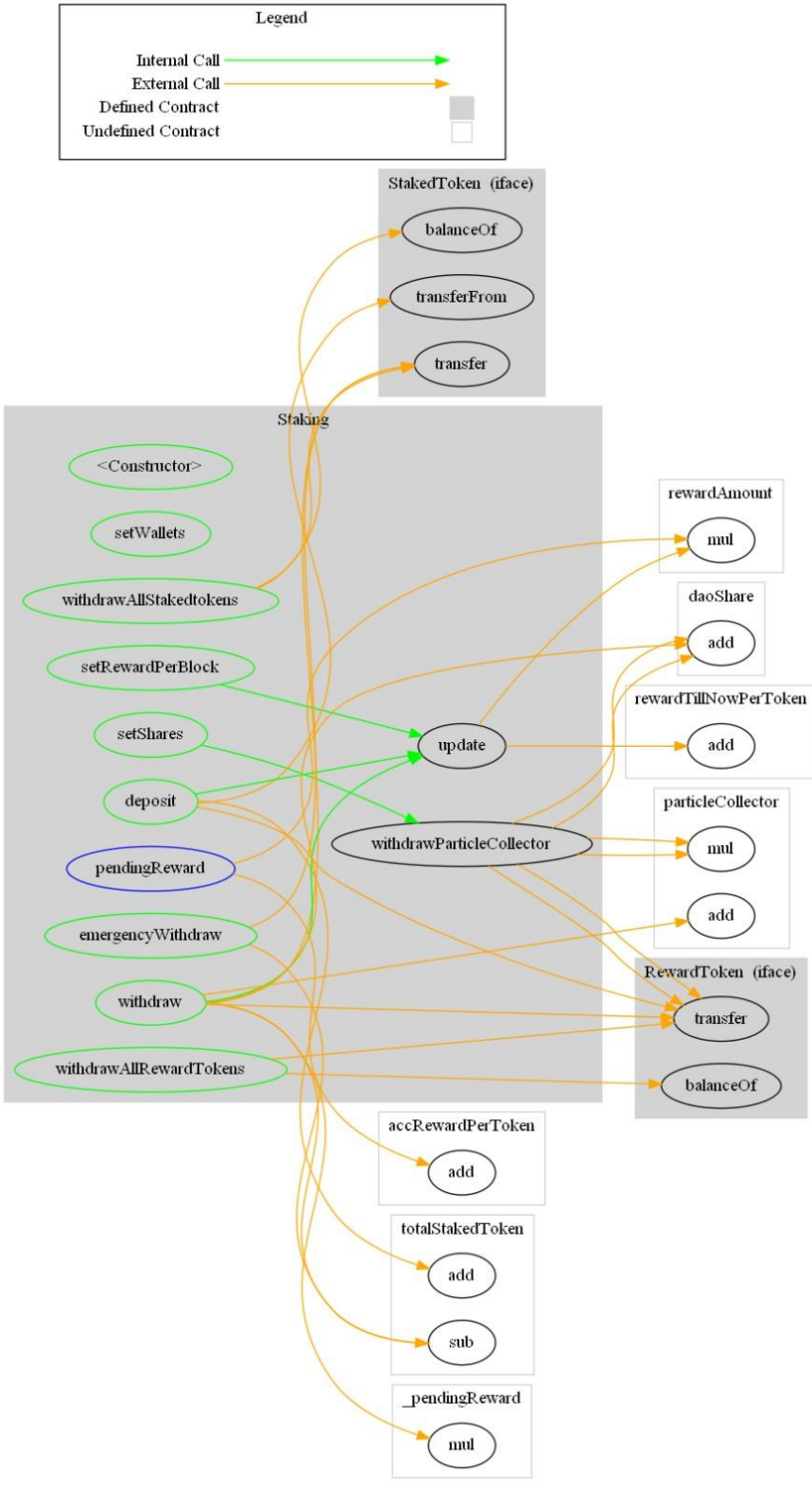
0xe054207b2f61b9fbd82f6986a7e8b16462f41b76002e9f6c6fce43220a4b6e9c

Deus Finance DAO link: https://client.aragon.org/#/deus

Debugging snippet Deus-DEA:

status true Transaction mined and execution succeed
transaction hash
0xe054207b2f61b9fbd82f6986a7e8b16462f41b76002e9f6c6fce43220a4b6e9c
from 0x8b9C5d6c73b4d11a362B62Bd4B4d3E52AF55C630
to Staking.transferOwnership(address)
0x8Cd408279e966b7e7E1f0b9E5eD8191959d11a19
gas 30940 gas
transaction cost 30940 gas
hash
0xe054207b2f61b9fbd82f6986a7e8b16462f41b76002e9f6c6fce43220a4b6e9c
input 0xf2f...9bc0f
decoded input { "address newOwner":
"0xd9775d818FC23e07aC4b8eFd4C58972F7c59BC0f" }
decoded output -
logs [{ "from": "0x8Cd408279e966b7e7E1f0b9E5eD8191959d11a19", "topic":
"0x8be0079c531659141344cd1fd0a4f28419497f9722a3daafe3b4186f6b6457e0",
"event": "OwnershipTransferred", "args": { "0":
"0x8b9C5d6c73b4d11a362B62Bd4B4d3E52AF55C630", "1":
"0xd9775d818FC23e07aC4b8eFd4C58972F7c59BC0f", "previousOwner":
"0x8b9C5d6c73b4d11a362B62Bd4B4d3E52AF55C630", "newOwner":
"0xd9775d818FC23e07aC4b8eFd4C58972F7c59BC0f", "length": 2 } }]
value 0 wei

Contract Flow



Audit Team

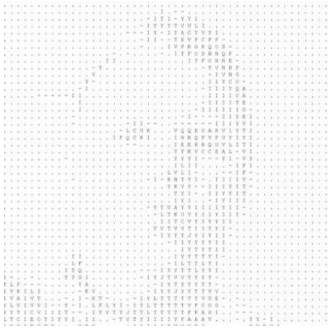
Team Lead: Eelko Neven

Eelko has been in the it/security space since 1991. His passion started when he was confronted with a formatted hard drive and no tools to undo it. At that point he started reading a lot of material on how computers work and how to make them work for others. After struggling for a few weeks he finally wrote his first HD data recovery program. Ever since then when he was faced with a challenge he just persisted until he had a solution.

This mindset helped him tremendously in the security space. He found several vulnerabilities in large corporation servers and notified these corporations in a responsible manner. Among those are Google, Twitter, General Electrics etc.

For the last 12 years he has been working as a professional security /code auditor and performed over 1500 security audits / code reviews, he also wrote a similar amount of reports.

He has extensive knowledge of the Solidity programming language and this is why he loves to do Defi and other smartcontract reviews.



Email:
info@coinbae.com

Conclusion

We performed the procedures as laid out in the scope of the audit and there were 11 findings, 8 medium and 3 low. There were also 3 high severity issues that were explained by the team in their response. Subsequently, these issues were removed by Coinbae, although still on the report for transparency's sake. The medium risk issues do not pose a security risk as they are best practice issues that is why the overall risk level is low.

Disclaimer

Coinbae audit is not a security warranty, investment advice, or an endorsement of the Deus Finance platform. This audit does not provide a security or correctness guarantee of the audited smart contracts. The statements made in this document should not be interpreted as investment or legal advice, nor should its authors be held accountable for decisions made based on them. Securing smart contracts is a multistep process. One audit cannot be considered enough. We recommend that the the Deus Finance Team put in place a bug bounty program to encourage further analysis of the smart contract by other third parties.