GEMZ

AUDIT REPORT

Security Report Prepared On
March 5 2021

APESWAPCODE REVIEW

TABLE OF CONTENTS

FARM

SWAP

SUMMARY

What follows is a code security audit of the ApeSwap project.

The information appearing in this report is for general purposes only and is not intended to provide any legal security guarantees to any individual or entity. It is advisable to conduct more reviews or/and audits as just one review or audit may miss important issues.

This report does not provide personalized investment advice or recommendations, nor does it provide advice to perform any transactions and it does not provide investment, financial, legal, or tax advice. We are not responsible or liable for any loss which results from the report. This report should not be considered as investment advice.

REPORT

FARM

BananaToken

Address: 0x603c7f932ED1fc6575303D8Fb018fDCBb0f39a95

The BANANA token's functionality is the same as Pancakeswap's CakeToken.

The owner of BananaToken is 0x5c8d727b265dbafaba67e050f2f739caeeb4a6f9 (MasterApe), and not an EOA. This means that only MasterApe can mint Banana tokens.

MasterApe

Address: 0x5c8D727b265DBAfaba67E050f2f739cAeEB4A6F9

There are two tokens involved, BANANA and BananaSplitBar (syrup). BANANA is the yield token distributed for depositing liquidity pair (LP) tokens, or staking the BANANA token. It appears that the purpose of BananaSplitBar is to act as the staking token for SupportApe.

The specified emission per block is 10 Banana tokens. This value has been initialized in the constructor upon contract creation and there is no code with functionality to change this value. However, the emission multiplier can be changed by the contract owner by changing the value of BONUS_MULTIPLIER using the updateMultiplier function. This can be observed from the first and second 72 hours bonus BANANA emission rates.

110% of the block emission is minted, with 100% (10) as the block rewards, and 10% (1) going to the dev address. The dev address is 0xcef34e4db130c8a64493517985b23af5b13e8cc6, and is an EOA. This is clarified in https://obiedobo.gitbook.io/apeswap-finance/the-usdbanana-frenzy.

The owner of the MasterApe contract is 0x2f07969090a2e9247c761747ea2358e5bb033460, which is a Timelock contract.

MasterApe Continued

getPoolInfo is an added view function that is used to read the pool information of a specified pool id.

A modifier named validatePool has been added to the following functions to ensure that the pid specified exists in the poolInfo array.

- updatePool
- deposit
- withdraw

A public view function named checkPoolDuplicate has been added, and is used in the add function, to check if a LP token address has already been registered in poolInfo.

The migrator and its migrate function has been removed.

SupportApe

Address: 0x54aff400858Dcac39797a81894D9920f16972D1D

The staking token is BananaSplitBar, which is minted by staking BANANA tokens in MasterApe.

There is no reward token emitted by this contract for staking. A user's balance is increased when deposit() is called to transfer tokens into the contract and decreased when withdraw() is called for the token to transfer the tokens back to the user. Calling emergencyWithdraw() withdraws all the user's deposited tokens and sets the user's balance in the contract to 0.

This contract does not appear to be currently used on ApeSwap.

REPORT

BananaSplitBar

Address: 0x86Ef5e73EDB2Fea111909Fe35aFcC564572AcC06

The BananaSplitBar token's functionality is the same as Pancakeswap's SyrupBar token.

The owner of BananaSplitBar is 0x5c8d727b265dbafaba67e050f2f739caeeb4a6f9 (MasterApe), and not an EOA. This means that only MasterApe can mint BananaSplitBar tokens.

MultiCall

Address: 0x38ce767d81de3940CFa5020B55af1A400ED4F657

The Multicall contract is used as a read-only contract for batching multiple read function calls from the frontend of the dapp. It is not used by any of the other contracts in the report.

Timelock

Address: 0x2F07969090a2E9247C761747EA2358E5bB033460

The Timelock contract is the same as the one used by Pancakeswap. The MINIMUM_DELAY is 6 hours (21600 seconds). The current timelock delay is set to 24 hours (86400 seconds). As this is the owner of the MasterApe contract, any onlyOwner function calls have to be queued through this contract for 24 hours before it can be executed.

BNBRewardApe

Address: 0x0245c697a96045183048cdf18e9abae5b2237ff6

Similar functionality as Pancakeswap's Smartchef contract (0x92E8CeB7eAeD69fB6E4d9dA43F605D2610214E68).

The staked token is BANANA, and the reward is native BNB (not WBNB). Hence, there are a few changes and additions made.

REPORT

BNBRewardApe Continued

depositBNBRewards is an external payable function. Anyone can send BNB to the contract and increase the contract’s BNB balance.

rewardBalance is a public view function which returns the BNB balance of the contract.

safeTransferBNB is an internal function used to transfer native BNB to an address. The external call to transfer is done with a gas limit of 23000.

The contract owner is able to withdraw an arbitrary amount of BNB, up to a maximum of the contract’s balance, from the contract using emergencyRewardWithdraw.

EXCHANGE

ApeFactory

Address: 0x0841BD0B734E4F5853f0dD8d7Ea041c241fb0Da6

Same functionality as Pancakeswap’s PancakeFactory contract (0xbcfccbde45ce874adcb698cc183debcf17952812).

ApeRouter

Address: 0xC0788A3aD43d79aa53B09c2EaCc313A787d1d607

Same functionality as Pancakeswap’s PancakeRouter contract (0x05ff2b0db69458a0750badebc4f9e13add608c7f).

ApePair

Address: 0xa0c3ef24414ed9c9b456740128d8e63d016a9e11

Same functionality as Pancakeswap’s LP token contract (e.g. 0x1b96b92314c44b159149f7e0303511fb2fc4774f).

RISK FACTORS

ISSUES

APE-001: BananaSplitBar is not burned when emergencyExit is called

<u>Severity: Low</u>

Similarly to the Pancakeswap Masterchef contract, there is an issue in the emergencyWithdraw, where the syrup.burn() is not called. Thus, it is possible for an account who has staked Banana into the pool with pid 0 to use emergencyExit to withdraw the staked Banana without burning any BananaSplitBar. This is done in the following steps:

- Call enterStaking to stake Banana. This will deposit the user's Banana and mint an equal amount of BananaSplitBar.
- Call emergencyWithdraw. The staked Banana will be returned, but BananaSplitBar is not burned.
- Repeat the 2 steps above.

This allows arbitrary minting of BananaSplitBar.
However, at the point of this audit, it appears that there is no usage of BananaSplitBar.

<u>Recommendations</u>

A fix for this would be to burn the same amount of BananaSplitBar as withdrawn BANANA when emergencyExit is called. However, this would require a redeployment of the MasterApe contract.

Note: The Apeswap team has acknowledged this issue and confirmed that BananaSplitBar will not be used as part of the dApp.

RISK FACTORS

ISSUES

ADDITIONAL RISKS

- APE-001 can be exploited to mint an arbitrary amount of BananaSplitBar tokens. If this BananaSplitBar token has a purpose in ApeSwap, a malicious actor can mint and inflate the number of BananaSplitBar and gain an unfair advantage over other users at staking or any other usages.

- The dev address receives approximately 9% of the actual emission of BANANA each block. As it is an EOA, the BANANA tokens can be moved at any time. At the point of this audit, the address is the top 6th holder of BANANA (https://bscscan.com/token/0x603c7f932ed1fc6575303d8fb018fdcbb0f39a95#balances)

RECOMMENDATIONS

- Due to APE-001, it is recommended that BananaSplitBar is never used for any purposes. It should also not be listed in the tokens list on Apeswap, and the ApeSwap team should make it clear that they do not encourage users to conduct trading of BananaSplitBar, and that it has no tangible value.

- Update the gitbook documentation to include contracts such as BNBRewardApe which are actually in use, and remove irrelevant contracts if they are not in use.

- Use a timelock for the address receiving the dev rewards.