Security Audit Report for Filda-DAO Smart Contracts

Date: Nov 4, 2022

Version: 1.0

Contact: contact@blocksec.com

BlockSec Audit Team

Digitally signed by BlockSec Audit Team
Date: 2022.11.04 12:13:14 +08'00'

Contents

Report Manifest

Item	Description
Client	FilDA
Target	Filda-DAO Smart Contracts

Version History

Version	Date	Description
1.0	Nov 4, 2022	First Release

About BlockSec BlockSec focuses on the security of the blockchain ecosystem and collaborates with leading DeFi projects to secure their products. BlockSec is founded by top-notch security researchers and experienced experts from both academia and industry. They have published multiple blockchain security papers in prestigious conferences, reported several zero-day attacks of DeFi applications, and successfully protected digital assets that are worth more than 5 million dollars by blocking multiple attacks. They can be reached at Email, Twitter and Medium.

Chapter 1 Introduction

1.1 About Target Contracts

Information	Description
Type	Smart Contract
Language	Solidity
Approach	Semi-automatic and manual verification

The target of this audit is the governance and reward component for the FilDA project. The original repository experienced a renaming, so the commit hash of the previous repository will be marked with * for clarity.

Repo Name	Github URL
Torches-dao	https://github.com/TorchesFinance/torches-dao*
FilDA-dao	https://github.com/fildaio/filda-dao

The auditing process is iterative. Specifically, we would audit the commits that fix the discovered issues. If there are new issues, we will continue this process. The commit SHA values during the audit are shown in the following table. Our audit report is responsible for the code in the initial version (Version 1), as well as new code (in the following versions) to fix issues in the audit report.

Project	Version	Commit Hash
Torches-dao	Version 1	e785cb8208ae2a8a34c7799a0b5cb2668e0ded68 *
FilDA-dao	Version 2	e810174a34616c27c4daa239e6f9e6f2d8790964

1.2 Disclaimer

This audit report does not constitute investment advice or a personal recommendation. It does not consider, and should not be interpreted as considering or having any bearing on, the potential economics of a token, token sale or any other product, service or other asset. Any entity should not rely on this report in any way, including for the purpose of making any decisions to buy or sell any token, product, service or other asset.

This audit report is not an endorsement of any particular project or team, and the report does not guarantee the security of any particular project. This audit does not give any warranties on discovering all security issues of the smart contracts, i.e., the evaluation result does not guarantee the nonexistence of any further findings of security issues. As one audit cannot be considered comprehensive, we always recommend proceeding with independent audits and a public bug bounty program to ensure the security of smart contracts.

The scope of this audit is limited to the code mentioned in Section 1.1. Unless explicitly specified, the security of the language itself (e.g., the solidity language), the underlying compiling toolchain and the computing infrastructure are out of the scope.

1.3 Procedure of Auditing

We perform the audit according to the following procedure.

- **Vulnerability Detection** We first scan smart contracts with automatic code analyzers, and then manually verify (reject or confirm) the issues reported by them.
- **Semantic Analysis** We study the business logic of smart contracts and conduct further investigation on the possible vulnerabilities using an automatic fuzzing tool (developed by our research team). We also manually analyze possible attack scenarios with independent auditors to cross-check the result.
- **Recommendation** We provide some useful advice to developers from the perspective of good programming practice, including gas optimization, code style, and etc.

We show the main concrete checkpoints in the following.

1.3.1 Software Security

* Reentrancy
* DoS
* Access control
* Data handling and data flow
* Exception handling
* Untrusted external call and control flow
* Initialization consistency
* Events operation
* Error-prone randomness
* Improper use of the proxy system

1.3.2 DeFi Security

* Semantic consistency
* Functionality consistency
* Permission management
* Business logic
* Token operation
* Emergency mechanism
* Oracle security
* Whitelist and blacklist
* Economic impact
* Batch transfer

1.3.3 NFT Security

* Duplicated item
* Verification of the token receiver
* Off-chain metadata security

1.3.4 Additional Recommendation

* Gas optimization
* Code quality and style

Note *The previous checkpoints are the main ones. We may use more checkpoints during the auditing process according to the functionality of the project.*

1.4 Security Model

To evaluate the risk, we follow the standards or suggestions that are widely adopted by both industry and academy, including OWASP Risk Rating Methodology [1] and Common Weakness Enumeration [2]. The overall *severity* of the risk is determined by *likelihood* and *impact*. Specifically, likelihood is used to estimate how likely a particular vulnerability can be uncovered and exploited by an attacker, while impact is used to measure the consequences of a successful exploit.

In this report, both likelihood and impact are categorized into two ratings, i.e., *high* and *low* respectively, and their combinations are shown in Table 1.1.

Table 1.1: Vulnerability Severity Classification

Impact \ Likelihood	*High*	*Low*
High	High	Medium
Low	Medium	Low

Accordingly, the severity measured in this report are classified into three categories: **High**, **Medium**, **Low**. For the sake of completeness, **Undetermined** is also used to cover circumstances when the risk cannot be well determined.

Furthermore, the status of a discovered item will fall into one of the following four categories:

- **Undetermined** No response yet.
- **Acknowledged** The item has been received by the client, but not confirmed yet.
- **Confirmed** The item has been recognized by the client, but not fixed yet.
- **Fixed** The item has been confirmed and fixed by the client.

[1] https://owasp.org/www-community/OWASP_Risk_Rating_Methodology

[2] https://cwe.mitre.org/

Chapter 2 Findings

In total, we find **five** potential issues.

- High Risk: 0
- Medium Risk: 4
- Low Risk: 1
- Recommendations: 0
- Notes: 0

ID	Severity	Description	Category	Status
1	Medium	Potential access control problem in the `VotingEscrow` contract	Software Security	Fixed
2	Medium	Potential price manipulation on the reward allocation speed	DeFi Security	Fixed
3	Medium	Delayed updates of voting powers in the `LiquidityGaugeV3` contract	DeFi Security	Undetermined
4	Medium	Accouting update problem in the `LiquidityGaugeV3` contract	DeFi Security	Fixed
5	Low	Potential inconsistent epoch length in the `LiquidityGaugeV3` contract	DeFi Security	Acknowledged

The details are provided in the following sections.

2.1 Software Security

2.1.1 Potential access control problem in the `VotingEscrow` contract

Severity Medium

Status Fixed in `Version 2`

Introduced by `Version 1`

Description

There is a potential access control bug in the `deposit_for` function of the `VotingEscrow` contract. As a premise, the `VotingEscrow` contract is designed for users locking their FILDA tokens (i.e., the reward and governance token of the Protocol) in exchange for the voting power. However, anyone is able to lock the FILDA tokens of other users (i.e., the victims in the following context) through the `deposit_for` function, if the following requirements are met:

- The victims have FILDA tokens.
- The victims have approved enough allowance of the FILDA tokens to the `VotingEscrow` contract.
- The victims have created locks in the `VotingEscrow` contract, and the locks haven't expired.

Under such circumstance, anyone could invoke the `deposit_for` function to lock any outstanding FILDA token holdings of the victims.

```
@external
@nonreentrant('lock')
def deposit_for(_addr: address, _value: uint256):
    """
```

```
    @notice Deposit ‘_value‘ tokens for ‘_addr‘ and add to the lock
    @dev Anyone (even a smart contract) can deposit for someone else, but
         cannot extend their locktime and deposit for a brand new user
    @param _addr User’s wallet address
    @param _value Amount to add to user’s lock
    """
    _locked: LockedBalance = self.locked[_addr]

    assert _value > 0 # dev: need non-zero value
    assert _locked.amount > 0, "No existing lock found"
    assert _locked.end > block.timestamp, "Cannot add to expired lock. Withdraw"

    self._deposit_for(_addr, _value, 0, self.locked[_addr], DEPOSIT_FOR_TYPE)
```

Listing 2.1: VotingEscrow.vy

Note that the above problem may become more serious due to the reward-claiming mechanism of this project. Specifically, in the `claim_rewards_for` function of the `RewardHelper` contract, anyone could arbitrarily claim rewards for other users. Though the rewards are always claimed into the correct accounts, the insufficient access control may cause a problem of calculating the reward amounts.

```
@external
def claim_rewards_for(_addr: address, _gauges: address[10]):
    """
    @notice Claim available reward tokens for ‘_addr‘
    @param _addr Address to claim for
    @param _gauges Gauge addresses to claim rewards
    """
    assert _addr != ZERO_ADDRESS, "invalid parameter"

    controller: address = self.controller
    minter: address = self.minter
    for gauge in _gauges:
        # check gauge is added
        if gauge != ZERO_ADDRESS and Controller(controller).gauge_types(gauge) >= 0:
            Minter(minter).mint_for(gauge, _addr)
            LiquidityGauge(gauge).claim_rewards(_addr)
```

Listing 2.2: RewardHelper.vy

Hence the `claim_rewards_for` function would affect the checkpoints recorded in the `LiquidityGaugeV3` contract. If the reward-claiming procedure can be controlled by others, the amount of the rewards may be different and may cause losses to the users. As a result, anyone can lock not only the FILDA tokens held by someone but also the rewards can be claimed.

Impact Arbitrarily claiming rewards for any users may affect the reward calculation and cause potential losses to the users.

Impact FILDA tokens can be locked in the `VotingEscrow` contract by any other users.

Suggestion Allow users to set a whitelist for delegating token locking.

2.2 DeFi Security

2.2.1 Potential price manipulation on the reward allocation speed

Severity Medium

Status Fixed in `Version 2`

Introduced by `Version 1`

Description There exists a price manipulation problem in the `_checkpoint` function of the `LiquidityGaugeV3` contract. The project provides incentives to the holders of `fToken`s (a series of Compound-CToken-like tokens) by adopting a mechanism similar to the Curve DAO project. Every time the function is invoked, a checkpoint is recorded for allocating the rewards.

Specifically, every balance change of `fToken`s would trigger a hook calling to the corresponding `LiquidityGaugeV3` contract and accumulate the reward in FILDA tokens. This hook updates the reward allocation points (points for short) based on the following two-step calculation:

1. The reward allocation speed for a certain time t is calculated as $r(t) = p * s(t)/WEEK$, where p is a system parameter, $s(t)$ is the total supply of `fToken` **recorded in the first checkpoint of a week**, $WEEK$ is the total seconds in a week (604800).
2. The points of a certain user is calculated as $I_u = \int \frac{r(t)b_u(t)}{s(t)}$, where $b_u(t)$ is the balance of the user at time t, and $s(t)$ is the current total supply of `fToken`.

In the actual implementation, the reward allocation speed $r(t)$ is only updated once per week. If there is no checkpoint in a whole week, then the $r(t)$ of the previous period is used. Therefore, there exists a path that malicious actors can use the flashloan to manipulate the reward allocation rates:

1. At the beginning of a week, borrowing the flashloan, and depositing underlying tokens to mint the corresponding `fToken`. This process would increase the `totalSupply` of `fToken`.
2. Since the `new_rate` calculation happens after updating the `totalSupply` of `fToken`, creating a checkpoint by calling functions like `user_checkpoint`. The creation of the checkpoint would **increase the recorded reward rate** thus further biases the reward allocation speed.
3. Redeeming `fToken` deposited to repay the flashloan.

The above steps may lead to biased reward allocation speed which would increase the amount of rewards for the current epoch.

```
@internal
def _checkpoint(addr: address):
    """
    @notice Checkpoint for a user
    @param addr User address
    """
    _point_period: int128 = self.point_period
    _point_period_timestamp: uint256 = self.point_period_timestamp[_point_period]
    _point_integrate_inv_supply: uint256 = self.point_integrate_inv_supply[_point_period]

    rate: uint256 = self.point_rate
    prev_epoch: uint256 = self.point_current_epoch_time
    new_rate: uint256 = rate
    next_epoch: uint256 = prev_epoch + WEEK

```

```
    if block.timestamp > next_epoch:
        new_totalSupply: uint256 = ERC20(self.lp_token).totalSupply()
        if new_totalSupply > 0:
            new_rate = self.point_proportion * new_totalSupply / WEEK
        self.point_current_epoch_time = next_epoch
        self.point_rate = new_rate

    # Update integral of 1/supply
    if block.timestamp > _point_period_timestamp and not self.is_killed:
        prev_week_time: uint256 = _point_period_timestamp
        week_time: uint256 = min((_point_period_timestamp + WEEK) / WEEK * WEEK, block.timestamp)
        _totalSupply: uint256 = self.lpTotalSupply

        for i in range(500):
            dt: uint256 = week_time - prev_week_time
            if _totalSupply > 0:
                if next_epoch >= prev_week_time and next_epoch < week_time:
                    # If we went across epoch, apply the rate
                    # of the first epoch until it ends, and then the rate of
                    # the last epoch.
                    _point_integrate_inv_supply += rate * (next_epoch - prev_week_time) /
                        _totalSupply
                    rate = new_rate
                    _point_integrate_inv_supply += rate * (week_time - next_epoch) / _totalSupply
```

Listing 2.3: LiquidityGaugeV3.vy

```
@external
def user_checkpoint(addr: address) -> bool:
    """
    @notice Record a checkpoint for ‘addr‘
    @param addr User address
    @return bool success
    """
    assert (msg.sender == addr) or (msg.sender == self.minter) # dev: unauthorized
    self._checkpoint(addr)
    self._checkpoint_dao(addr)
    self._checkpoint_rewards(addr, False, ZERO_ADDRESS)
    self._update_liquidity_limit(addr, self._balance_of(addr), self.totalSupply)
    return True
```

Listing 2.4: LiquidityGaugeV3.vy

Impact The calculation of the reward allocation speed can be manipulated by using the flashloan.

Suggestion Check the rate updating mechanism.

2.2.2 Delayed updates of voting powers in the `LiquidityGaugeV3` contract

Severity Medium

Status Undetermined

Introduced by `Version 1`

Description In the LiquidityGaugeV3 contract, the reward distribution calculation involves the working_balance variable of users. A user's working_balance is calculated as follows:

$$B = \min(I, 0.4I + 0.6S\frac{w}{W})$$

Here I is the current reward points of the user, S is the total reward points recorded in a variable named working_supply, while w and W represent the voting power the user holds and the total voting power recorded in the VotingEscrow contract, respectively.

If users do not update their voting power in the VotingEscrow contract, the corresponding w and W will decrease at the same speed, so the ratio of the user's voting power to the total voting power (i.e., w/W) remains the same. If there are other users locking FILDA tokens in the VotingEscrow contract, the total voting power would increase, which means the ratio a certain user would decrease. However, if the _update_liquidity_limit function is not invoked, the ratio will not be modified.

In summary, if users lock FILDA tokens in the VotingEscrow contract, it would reduce the voting power ratio of all other users, but this decrease is not updated into the LiquidityGaugeV3 contract in time. It may lead to incorrect calculation of the reward amounts.

```
@internal
def _update_liquidity_limit(addr: address, l: uint256, L: uint256):
    """
    @notice Calculate limits which depend on the amount of CRV token per-user.
            Effectively it calculates working balances to apply amplification
            of CRV production by CRV
    @param addr User address
    @param l User's amount of liquidity (LP tokens)
    @param L Total amount of liquidity (LP tokens)
    """
    # To be called after totalSupply is updated
    _voting_escrow: address = self.voting_escrow
    voting_balance: uint256 = ERC20(_voting_escrow).balanceOf(addr)
    voting_total: uint256 = ERC20(_voting_escrow).totalSupply()

    lim: uint256 = l * TOKENLESS_PRODUCTION / 100
    if voting_total > 0:
        lim += L * voting_balance / voting_total * (100 - TOKENLESS_PRODUCTION) / 100

    lim = min(l, lim)
    old_bal: uint256 = self.working_balances[addr]
    self.working_balances[addr] = lim
    _working_supply: uint256 = self.working_supply + lim - old_bal
    self.working_supply = _working_supply

    log UpdateLiquidityLimit(addr, l, L, lim, _working_supply)
```

Listing 2.5: LiquidityGaugeV3.vy

Impact Delayed updates of the voting power ratio of the users may cause incorrect reward distribution.

Suggestion N/A

2.2.3 Accouting update problem in the `LiquidityGaugeV3` contract

Severity Medium

Status Fixed in Version 2

Introduced by Version 1

Description The `LiquidityGaugeV3` contract is implemented as a fork from the Curve Protocol with some modification. However, there exist some interdependencies of the variables that could cause accounting update problem due to the modification. Specifically, there are two functions, `_checkpoint_dao` and `_checkpoint_rewards`, that calculate rewards based on a variable named `working_supply`. If `working_supply` is updated without calling the corresponding checkpoint function, it would cause accounting update problem in the `LiquidityGaugeV3` contract, as follows:

1. In the `claim_rewards` function, the `_update_liquidity_limit` function is called without calling the `_checkpoint_dao` function. Because the former function updates `working_supply`, it would cause accounting problems.

```
@external
@nonreentrant('lock')
def claim_rewards(_addr: address = msg.sender, _receiver: address = ZERO_ADDRESS):
    """
    @notice Claim available reward tokens for `_addr`
    @param _addr Address to claim for
    @param _receiver Address to transfer rewards to - if set to
                     ZERO_ADDRESS, uses the default reward receiver
                     for the caller
    """
    if _receiver != ZERO_ADDRESS:
        assert _addr == msg.sender # dev: cannot redirect when claiming for another user
    self._checkpoint_rewards(_addr, True, _receiver)

    # update user's point amount and working balance
    self._checkpoint(_addr)
    self._update_liquidity_limit(_addr, self._balance_of(_addr), self.totalSupply)
```

Listing 2.6: LiquidityGaugeV3.vy

2. Similarly, the `user_checkpoint` function calls the `_update_liquidity_limit` function, but does not call the `_checkpoint_rewards` function. Hence it has the similar accounting problem.

```
@external
def user_checkpoint(addr: address) -> bool:
    """
    @notice Record a checkpoint for `addr`
    @param addr User address
    @return bool success
    """
    assert (msg.sender == addr) or (msg.sender == self.minter) # dev: unauthorized
    self._checkpoint(addr)
    self._checkpoint_dao(addr)
    self._update_liquidity_limit(addr, self._balance_of(addr), self.totalSupply)
    return True
```

Listing 2.7: LiquidityGaugeV3.vy

Impact Incorrect handling of the interdependencies of state variables may cause accounting problems.

Suggestion Revise the code.

2.2.4 Potential inconsistent epoch length in the `LiquidityGaugeV3` contract

Severity Low

Status Acknowledged

Introduced by `Version 1`

Description There exists a potential inconsistency in the `_checkpoint_dao` function of the `LiquidityGaugeV3` contract. Specifically, the epoch retrieved from `RewardPolicyMaker` (at line 302) is assumed to be the length of `WEEK` (which is the total seconds in a week, i.e., 604,800 seconds). However, in the `RewardPolicyMaker` contract, the epoch length may not be fixed. This inconsistency may bring unexpected results.

```
280 @internal
281 def _checkpoint_dao(addr: address):
282     """
283     @notice Checkpoint interest for a user
284     @param addr User address
285     """
286     _period: int128 = self.period
287     _period_time: uint256 = self.period_timestamp[_period]
288     _integrate_inv_supply: uint256 = self.integrate_inv_supply[_period]
289
290     _epoch: uint256 = RewardPolicyMaker(self.reward_policy_maker).epoch_at(block.timestamp)
291     if _period_time == 0:
292         _period_time = RewardPolicyMaker(self.reward_policy_maker).epoch_start_time(_epoch)
293
294     # Update integral of 1/supply
295     if block.timestamp > _period_time and not self.is_killed:
296         _working_supply: uint256 = self.working_supply
297         _controller: address = self.controller
298         Controller(_controller).checkpoint_gauge(self)
299         prev_week_time: uint256 = _period_time
300
301         for i in range(500):
302             _epoch = RewardPolicyMaker(self.reward_policy_maker).epoch_at(prev_week_time)
303             week_time: uint256 = RewardPolicyMaker(self.reward_policy_maker).epoch_start_time(
                    _epoch + 1)
304             week_time = min(week_time, block.timestamp)
305
306             dt: uint256 = week_time - prev_week_time
307             w: uint256 = Controller(_controller).gauge_relative_weight(self, prev_week_time / WEEK
                    * WEEK)
```

Listing 2.8: LiquidityGaugeV3.vy

Impact Inconsistent settings of the parameters may bring unexpected results.

Suggestion Make the configuration and the calculation consistent.

Feedback from the Developers We would make sure that the `epoch_length` parameter in the `RewardPolicyMaker` contract is properly set to one week in seconds.