Security Audit of VaultyFinance (merged final)

Conclusion

Audit was done by the “Web3Go” team https://web3go.tech/ (https://web3go.tech/)
by Vladimir Smelov vladimirfol@gmail.com (mailto:vladimirfol@gmail.com)
https://www.linkedin.com/in/vladimir-smelov-25021669/ (https://www.linkedin.com/in/vladimir-smelov-25021669/)

In the final contract were not found:

- Backdoors for investor funds withdrawal by anyone.
- Bugs allowing to steal money from the contract.
- Other security problems.

Obvious errors or backdoors were not found in the contract.
The client was acknowledged about all secutiry notes below.

SECURED 100% SECURED

Scope

https://github.com/VaultyFinance/contracts (https://github.com/VaultyFinance/contracts)
The audit was done in 3 stages:

- In the first audit the scope was in the comment `289b19252f150c13fa593c6add8563d383b5a17e` :

> All except contracts/nft/* and contracts/token/erc1155.sol

- In the second audit the scope was in the commit `3eac9b1cdf0749ed1be7b59178d2c3432751aae4` :

> nft folder + tokens Lantti + ERC1155

- In the third audit the scope was in the commit `622259f89005d253d951a6422642b4cee9a52a84` :

> strategies/alpaca
> GovernanceStaking.sol

Methodology

1. Blind audit. Try to understand the structure of the code.
2. Find info in internet.
3. Ask quiestions to developers.
4. Draw the scheme of cross-contracts interactions.
5. Write user-stories, usage cases.
6. Run static analyzers

Find problems with:

- backdoors
- bugs
- math
- potential leaking of funds
- potential locking of the contract
- validate arguments and events
- others

Result

Critical

Not found.

Major

1. Return value is ignored

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/NotifyHelper.sol#L52 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/NotifyHelper.sol#L52)
- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/NotifyHelper.sol#L73 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/NotifyHelper.sol#L73)
- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/NotifyHelper.sol#L88 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/NotifyHelper.sol#L88)
- https://github.com/VaultyFinance/contracts/blob/622259f89005d253d951a6422642b4cee9a52a84/GovernanceStaking.sol#L24 (https://github.com/VaultyFinance/contracts/blob/622259f89005d253d951a6422642b4cee9a52a84/GovernanceStaking.sol#L24)
- https://github.com/VaultyFinance/contracts/blob/622259f89005d253d951a6422642b4cee9a52a84/GovernanceStaking.sol#L33 (https://github.com/VaultyFinance/contracts/blob/622259f89005d253d951a6422642b4cee9a52a84/GovernanceStaking.sol#L33)
- https://github.com/VaultyFinance/contracts/blob/622259f89005d253d951a6422642b4cee9a52a84/GovernanceStaking.sol#L43 (https://github.com/VaultyFinance/contracts/blob/622259f89005d253d951a6422642b4cee9a52a84/GovernanceStaking.sol#L43)

Recommendation.

Use SafeERC20 library.

Status.

Fixed in several commits, so there is no such issue at commit `1584bee517fc8d47ac016a45c0f54114cd8b54c2`

2. Reentry in Governance controlled method.

If you have reentry inside `transfer` you can withdraw tokens any times you want.

```
    function withdrawTokens() public onlyGovernance {
      require(block.timestamp - depositTimestamp > lockPeriod, "too early");

      uint256 unavailableTokens = tokensStaked;
      uint256 availableTokens = tokensLocked - unavailableTokens;
      token.transfer(msg.sender, availableTokens);

      tokensLocked = unavailableTokens;
    }
```

Recommendation.

Change state before external call.

Status.

Fixed at `1584bee517fc8d47ac016a45c0f54114cd8b54c2`

3. Potentialy dangerous reentry.

LPTokenWrapper.sol:

```
      function stakeTokens(uint256 amount) internal {
          require(amount > 0, "Cannot stake 0");
          _totalSupply = _totalSupply.add(amount);
          _balances[msg.sender] = _balances[msg.sender].add(amount);
          lpToken.safeTransferFrom(msg.sender, address(this), amount);

          stakeTimestamp[msg.sender] = block.timestamp;
      }
```

you can call withdraw in reentry from safeTransferFrom

Recommendation.

Change state before external call.

Status.

Fixed at `1584bee517fc8d47ac016a45c0f54114cd8b54c2`

4. Potential front-running.

At

- https://github.com/VaultyFinance/contracts/blob/622259f89005d253d951a6422642b4cee9a52a84/strategies/alpaca/AlpacaBaseStrategy.sol#L134 (https://github.com/VaultyFinance/contracts/blob/622259f89005d253d951a6422642b4cee9a52a84/strategies/alpaca/AlpacaBaseStrategy.sol#L134)
- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/strategies/pancakeswap/PancakeMasterChefLPStrategy.sol#L175 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/strategies/pancakeswap/PancakeMasterChefLPStrategy.sol#L175)
- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/strategies/pancakeswap/PancakeMasterChefLPStrategy.sol#L201 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/strategies/pancakeswap/PancakeMasterChefLPStrategy.sol#L201)

and in various similar places.

`amountOutMin = 1` is too low. Any rate will be accepted, potentially weak for front-running.

Recommendation.

Add `amountOutMin` as an argument, let user to control it.

Status.

ACKNOWLEDGED

Warning

1. Address zero-check for attribute set.

At

- https://github.com/VaultyFinance/contracts/blob/622259f89005d253d951a6422642b4cee9a52a84/upgradability/BaseUpgradeableStrategyStorage.sol#L147 (https://github.com/VaultyFinance/contracts/blob/622259f89005d253d951a6422642b4cee9a52a84/upgradability/BaseUpgradeableStrategyStorage.sol#L147)
- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/FeeRewardForwarder.sol#L35 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/FeeRewardForwarder.sol#L35)
- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/FeeRewardForwarder.sol#L46

(https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/FeeRewardForwarder.sol#L46)

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/strategies/pancakeswap/PancakeMasterChefLPStrategy.sol#L39-43 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/strategies/pancakeswap/PancakeMasterChefLPStrategy.sol#L39-43)
- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/NotifyHelper.sol#L25-27 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/NotifyHelper.sol#L25-27)
- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/RewardDistributionRecipient.sol#L8 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/RewardDistributionRecipient.sol#L8)
- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/RewardDistributionRecipient.sol#L20 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/RewardDistributionRecipient.sol#L20)
- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/NotifyHelper.sol#L38 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/NotifyHelper.sol#L38) here even we could add interface validation.
- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/NotifyHelper.sol#L96 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/NotifyHelper.sol#L96)

it’s not checked that the address is not 0.
It may be broken in front-end.

Recommendation.

Add

```
require(_address != address(0), "ZERO_ADDRESS");
```

Status.

ACKNOWLEDGED

2. Use SafeMath or solidity ^0.8.0.

There are a lot of places where you do unsafe substraction.
It’s easy to miss a mistake.
Especially these places look dangerous:

- https://github.com/VaultyFinance/contracts/blob/622259f89005d253d951a6422642b4cee9a52a84/GovernanceStaking.sol#L32 (https://github.com/VaultyFinance/contracts/blob/622259f89005d253d951a6422642b4cee9a52a84/GovernanceStaking.sol#L32)

Recommendation.

Use SafeMath everywhere or solidity ^0.8.0.

Status.

Fixed at `1584bee517fc8d47ac016a45c0f54114cd8b54c2` , SafeMath was used.

3. Potential place to make a mistake of usage.

- https://github.com/VaultyFinance/contracts/blob/622259f89005d253d951a6422642b4cee9a52a84/GovernanceStaking.sol#L38 (https://github.com/VaultyFinance/contracts/blob/622259f89005d253d951a6422642b4cee9a52a84/GovernanceStaking.sol#L38)
- https://github.com/VaultyFinance/contracts/blob/622259f89005d253d951a6422642b4cee9a52a84/GovernanceStaking.sol#L49 (https://github.com/VaultyFinance/contracts/blob/622259f89005d253d951a6422642b4cee9a52a84/GovernanceStaking.sol#L49)

you pass pool to stake and reset the pool, but not require unstake to call before, what may lead to loose tokens.
Note, that inside unstake you have requirement to unstake amount > 0, so ignore unstake in this case, otherwise the transaction will fail.

Status.

ACKNOWLEDGED

4. Too big contract.

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/Vault.sol (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/Vault.sol)

```
Warning: Contract code size exceeds 24576 bytes
(a limit introduced in Spurious Dragon).
This contract may not be deployable on mainnet.
Consider enabling the optimizer (with a low "runs" value!),
turning off revert strings, or using libraries.
```

Recommendation.

Resolve the warning.

Status.

ACKNOWLEDGED

5. Reentry on alreadyNotified (but adminOnly)

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/NotifyHelper.sol#L54 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/NotifyHelper.sol#L54)

`alreadyNotified[pools[i]] = true;` set after external call, this allow reentry.

Also this place seems dangerous:

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/NotifyHelper.sol#L76 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/NotifyHelper.sol#L76)

Recommendation.

Add noReentry modifier.

Status.

ACKNOWLEDGED

Comment

1. Place SPDX license comment everywhere.

Compiler gives warnings.

```
Warning: SPDX license identifier not provided in source file.
Before publishing, consider adding a comment containing
"SPDX-License-Identifier: <SPDX-License>" to each source file.
Use "SPDX-License-Identifier: UNLICENSED" for non-open-source code.
Please see https://spdx.org for more information.
```

Recommendation.

Place license.

Status.

NOT_ISSUE
ACKNOWLEDGED

2. Shadows other declarations

From the Slither logs for `622259f89005d253d951a6422642b4cee9a52a84`:

```
ControllableInit.sol#11 shadows:
GovernableInit.sol#37-43

strategies/alpaca/AlpacaBaseStrategy.sol#45 shadows:
GovernableInit.sol#37-43

strategies/alpaca/AlpacaETHStrategy.sol#12 shadows:
GovernableInit.sol#37-43

strategies/alpaca/AlpacaETHStrategy.sol#15 shadows:
upgradability/BaseUpgradeableStrategyStorage.sol#44-46
```

Recommendation.

Do not shadow declarations, it’s dangerous to misuse variable/method.

Status.

NOT_ISSUE
ACKNOWLEDGED

3. Methods should be declared external.

Everywhere where method is used only externaly (never internaly) it’s better to set modifer to `external` not `public` to save gas.

Recommendation.

Make methods `external` to save gas.

Status.

NOT_ISSUE
ACKNOWLEDGED

4. Use reentryGuard.

Use reentryGuard on every external/public method to be sure no reentry will happen.

Recommendation.

Use reentryGuard.

Status.

NOT_ISSUE
ACKNOWLEDGED

5. Lack of events.

You don’t have much events. It will be difficult to monitor the contract activity.
e.g.

- https://github.com/VaultyFinance/contracts/blob/622259f89005d253d951a6422642b4cee9a52a84/strategies/alpaca/AlpacaBaseStrategy.sol#L100 (https://github.com/VaultyFinance/contracts/blob/622259f89005d253d951a6422642b4cee9a52a84/strategies/alpaca/AlpacaBaseStrategy.sol#L100)

- https://github.com/VaultyFinance/contracts/blob/622259f89005d253d951a6422642b4cee9a52a84/strategies/alpaca/AlpacaBaseStrategy.sol#L107 (https://github.com/VaultyFinance/contracts/blob/622259f89005d253d951a6422642b4cee9a52a84/strategies/alpaca/AlpacaBaseStrategy.sol#L107)

- https://github.com/VaultyFinance/contracts/blob/622259f89005d253d951a6422642b4cee9a52a84/strategies/alpaca/AlpacaBaseStrategy.sol#L112 (https://github.com/VaultyFinance/contracts/blob/622259f89005d253d951a6422642b4cee9a52a84/strategies/alpaca/AlpacaBaseStrategy.sol#L112)

- https://github.com/VaultyFinance/contracts/blob/622259f89005d253d951a6422642b4cee9a52a84/GovernanceStaking.sol#L45 (https://github.com/VaultyFinance/contracts/blob/622259f89005d253d951a6422642b4cee9a52a84/GovernanceStaking.sol#L45)

- https://github.com/VaultyFinance/contracts/blob/622259f89005d253d951a6422642b4cee9a52a84/GovernanceStaking.sol#L51 (https://github.com/VaultyFinance/contracts/blob/622259f89005d253d951a6422642b4cee9a52a84/GovernanceStaking.sol#L51)

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/LPTokenWrapper.sol#L33 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/LPTokenWrapper.sol#L33)

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/LPTokenWrapper.sol#L30 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/LPTokenWrapper.sol#L30)

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/RewardDistributionRecipient.sol#L20 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/RewardDistributionRecipient.sol#L20)

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/NotifyHelper.sol#L96 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/NotifyHelper.sol#L96)

Recommendation.

Add events with interesting argument, don’t foreget about indexes.

Status.

NOT_ISSUE
ACKNOWLEDGED

6. Compilation-time const calculation

At

- https://github.com/VaultyFinance/contracts/blob/622259f89005d253d951a6422642b4cee9a52a84/strategies/alpaca/AlpacaBaseStrategy.sol (https://github.com/VaultyFinance/contracts/blob/622259f89005d253d951a6422642b4cee9a52a84/strategies/alpaca/AlpacaBaseStrategy.sol)
  you can just write compilation-time calculations instead of unclear hash (and then testing in constructor).

Recommendation.

Calculate const at compilation time using statement.

Status.

NOT_ISSUE
ACKNOWLEDGED

7. Deflation tokens support.

This is not true for all tokens, that after `transfer(x)` balance will change for `x` tokens, because some contracts burn some tokens on every transfer. There were some hacks in DeFi based on this fact.

This is a valid note for all contracts which use any ERC20/BEP20 tokens.

Recommendation.

Check balances after transfer or add a comment note that such tokens are not supported.

Status.

NOT_ISSUE
ACKNOWLEDGED

8. Duplicated modifier.

At

- https://github.com/VaultyFinance/contracts/blob/622259f89005d253d951a6422642b4cee9a52a84/strategies/alpaca/AlpacaBaseStrategy.sol#L165 (https://github.com/VaultyFinance/contracts/blob/622259f89005d253d951a6422642b4cee9a52a84/strategies/alpaca/AlpacaBaseStrategy.sol#L165)
  you don’t need the modifier `onlyNotPausedInvesting` since the only usage is at the

- https://github.com/VaultyFinance/contracts/blob/622259f89005d253d951a6422642b4cee9a52a84/strategies/alpaca/AlpacaBaseStrategy.sol#L243 (https://github.com/VaultyFinance/contracts/blob/622259f89005d253d951a6422642b4cee9a52a84/strategies/alpaca/AlpacaBaseStrategy.sol#L243)
  and you already have this check.

Recommendation.

Check all requirements in external methods and rely on pre-conditions insider internal methods.

Status.

NOT_ISSUE
ACKNOWLEDGED

9. Magic const.

At

- https://github.com/VaultyFinance/contracts/blob/622259f89005d253d951a6422642b4cee9a52a84/strategies/alpaca/AlpacaBNBStrategy.sol:24 (https://github.com/VaultyFinance/contracts/blob/622259f89005d253d951a6422642b4cee9a52a84/strategies/alpaca/AlpacaBNBStrategy.sol:24)
  you have unclear magic const.

Recommendation.

Do not use magic unnamed const.
Better use arguments or at least contract level named constants.

Status.

NOT_ISSUE
ACKNOWLEDGED

10. Hardcoded params.

Several places like:

```
    address underlying = address(0x7130d2A12B9BCbFAe4f2634d864A1Ee1Ce3Ead9c);
    address wbnb = address(0xbb4CdB9CBd36B01bD1cBaEBF2De08d9173bc095c);
    address alpaca = address(0x8F0528cE5eF7B51152A59745bEfDD91D97091d2F);
    address ibToken = address(0xe124118Cf775D320C11319458A9836a092E24307);
```

```
            90, // profit sharing numerator  //xx why not vars
            1000, // profit sharing denominator
            true, // sell
            1e16, // sell floor
            12 hours // implementation change delay  //xx too small
```

Recommendation.

Pass them as arguments.
More flexible for testing and deployments to other chains.

Status.

NOT_ISSUE
ACKNOWLEDGED

11. Too small implementation delay.

At:

- https://github.com/VaultyFinance/contracts/blob/622259f89005d253d951a6422642b4cee9a52a84/strategies/alpaca/AlpacaBaseStrategy.sol:62 (https://github.com/VaultyFinance/contracts/blob/622259f89005d253d951a6422642b4cee9a52a84/strategies/alpaca/AlpacaBaseStrategy.sol:62)
  you set implementation delay to 12 hours what is small for users.

Recommendation.

Think about increment (~48h).

Status.

NOT_ISSUE
ACKNOWLEDGED

12. Require correct path.

At

- https://github.com/VaultyFinance/contracts/blob/622259f89005d253d951a6422642b4cee9a52a84/strategies/alpaca/AlpacaBaseStrategy.sol:111 (https://github.com/VaultyFinance/contracts/blob/622259f89005d253d951a6422642b4cee9a52a84/strategies/alpaca/AlpacaBaseStrategy.sol:111)
  you check for the first path symbol but not for the last.

Recommendation.

Add

```
require(_route[_route.length-1] == .., "Path should end with ...");
```

Status.

NOT_ISSUE
ACKNOWLEDGED

13. Require contract initialized.

In strategies/alpaca/AlpacaBaseStrategy.sol
you use `pancake_route` but it may be not initialize yet, as well as other arguments.

Recommendation.

Require the contract to be fully initialized before work with it.

Status.

NOT_ISSUE
ACKNOWLEDGED

14. Event argument is always false.

The 2nd argument of `ProfitsNotCollected` is always false in all usages.

Recommendation.

Remove second argument, or (better) replace it with several others.

Status.

NOT_ISSUE
ACKNOWLEDGED

15. Return value is ignored of swapExactTokensForTokens

At

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/FeeRewardForwarder.sol#L123

(https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/FeeRewardForwarder.sol#L123)

The return value of the method call is ignored.

Recommendation.

According to the interface you should check if return swap result equals to expected.

Status.

ACKNOWLEDGED

16. Follow the language naming style.

At

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/FeeRewardForwarder.sol#L18 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/FeeRewardForwarder.sol#L18)
- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/FeeRewardForwarder.sol#L19 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/FeeRewardForwarder.sol#L19)
- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/FeeRewardForwarder.sol#L22 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/FeeRewardForwarder.sol#L22)
- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/FeeRewardForwarder.sol#L30 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/FeeRewardForwarder.sol#L30)
- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/Controller.sol#L38 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/Controller.sol#L38)
- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/Controller.sol#L39 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/Controller.sol#L39)

const are not in UPPER_CASE

At

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/Migrations.sol#L5 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/Migrations.sol#L5)

attributes are not in camelCase

Recommendation.

Follow the language naming style.

Status.

NOT_ISSUE
ACKNOWLEDGED

17. Better naming.

At

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/FeeRewardForwarder.sol#L47 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/FeeRewardForwarder.sol#L47)
  better to use `ProfitSharingPoolSet` name for the event.

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/strategies/pancakeswap/PancakeMasterChefLPStrategy.sol#L26 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/strategies/pancakeswap/PancakeMasterChefLPStrategy.sol#L26)
  use `_REWARD_POOL_ID_SLOT`

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/Controllable.sol#L5 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/Controllable.sol#L5)
  use `ControllableGovernable`

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/LPTokenWrapper.sol#L16 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/LPTokenWrapper.sol#L16)
  use `withdrawFeeBeforeDelay` , since after delay there is not fee.

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/LPTokenWrapper.sol#L44 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/LPTokenWrapper.sol#L44)
  use `lastStakeTimestamp`.

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/Storage.sol#L3 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/Storage.sol#L3)
  use `StorageGovernanceController`

Recommendation.

Use self-explainable names.

Status.

NOT_ISSUE
ACKNOWLEDGED

18. Poor comments.

At

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/LPTokenWrapper.sol#L7 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/LPTokenWrapper.sol#L7)
  the purpose of the contract is not clear from the first sight and from the second :-)

At

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/NotifyHelper.sol (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/NotifyHelper.sol)
  the purpose is not clear

… a lot of unclear places in the code …

Recommendation.

Add docstrings and comments.

Status.

NOT_ISSUE
ACKNOWLEDGED

19. Potential events misordering.

At

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/Controller.sol#L109 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/Controller.sol#L109)
- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/NoMintRewardPool.sol#L153 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/NoMintRewardPool.sol#L153)
- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/NoMintRewardPool.sol#L157 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/NoMintRewardPool.sol#L157)
- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/NoMintRewardPool.sol#L178 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/NoMintRewardPool.sol#L178)
- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/NoMintRewardPool.sol#L195 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/NoMintRewardPool.sol#L195)
- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/Vault.sol#L225 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/Vault.sol#L225)
- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/interfaces/Vault.sol#L248 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/interfaces/Vault.sol#L248)
- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/interfaces/Vault.sol#L299 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/interfaces/Vault.sol#L299)

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/interfaces/Vault.sol#L318 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/interfaces/Vault.sol#L318)

Emit event before external call.
Potential mis-ordering.

Recommendation.

Be careful on frontEnd. Use noReentrant.

Status.

NOT_ISSUE
ACKNOWLEDGED

20. Attritubte redefined in constructor

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/FeeRewardForwarder.sol#L27 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/FeeRewardForwarder.sol#L27)

Recommendation.

Replace with `address public targetToken;`

Status.

NOT_ISSUE
ACKNOWLEDGED

21. Indexed event attribute

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/FeeRewardForwarder.sol#L32 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/FeeRewardForwarder.sol#L32)

Recommendation.

Add indexation.

Status.

NOT_ISSUE
ACKNOWLEDGED

22. Unused variable

At

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/FeeRewardForwarder.sol#L75 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/FeeRewardForwarder.sol#L75)
  makes no sense to set to new var since it never changes.

At

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/upgradability/BaseUpgradeabilityProxy.sol#L31 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/upgradability/BaseUpgradeabilityProxy.sol#L31)

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/upgradability/BaseUpgradeabilityProxy.sol#L53 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/upgradability/BaseUpgradeabilityProxy.sol#L53)

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/NotifyHelper.sol#L45 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/NotifyHelper.sol#L45)

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/NotifyHelper.sol#L68 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/NotifyHelper.sol#L68)

you can use const inside ASM.

At

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/NoMintRewardPool.sol#L75 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/NoMintRewardPool.sol#L75) the veriable does not affect any logic.

Recommendation.

Do not use unused variables.

Status.

NOT_ISSUE
ACKNOWLEDGED

23. Replace if/else-revert with require

At

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/FeeRewardForwarder.sol#L113 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/FeeRewardForwarder.sol#L113)
  it’s better to decrease levels of the code and be more exact to use one require at the top.

The same for

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/strategies/pancakeswap/PancakeMasterChefLPStrategy.sol#L172 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/strategies/pancakeswap/PancakeMasterChefLPStrategy.sol#L172)

Recommendation.

Replace with `require` .

Status.

NOT_ISSUE
ACKNOWLEDGED

24. Misnaming in comment.

At

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/ControllableInit.sol#L5 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/ControllableInit.sol#L5)

Recommendation.

Replace

```
  // A clone of Governable supporting the Initializable interface and pattern
```

with

```
  // A clone of Controllable supporting the Initializable interface and pattern
```

Status.

NOT_ISSUE
ACKNOWLEDGED

25. Shadows other declarations

At

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/ControllableInit.sol#L11 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/ControllableInit.sol#L11)
  shadows - GovernableInit._storage()

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/VaultProxy.sol#L8 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/VaultProxy.sol#L8)
  shadows upgradability/BaseUpgradeabilityProxy.sol#30-35)

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/Vault.sol#L33-37 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/Vault.sol#L33-37)

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/Vault.sol#L52 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/Vault.sol#L52)
  shadows Vault.underlyingUnit()

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/VaultStorage.sol#L38-43 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/VaultStorage.sol#L38-43)
  shadows VaultStorage._underlying() (VaultStorage.sol#69-71)
  shadows VaultStorage._underlyingUnit() (VaultStorage.sol#77-79)

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/Vault.sol#L170 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/Vault.sol#L170)
  shadows VaultStorage._strategy() (VaultStorage.sol#61-63)

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/Vault.sol#L180 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/Vault.sol#L180)
  shadows VaultStorage._strategy() (VaultStorage.sol#61-63)

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/Vault.sol#L196 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/Vault.sol#L196)
  shadows VaultStorage._strategy() (VaultStorage.sol#61-63)

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/Vault.sol#L276 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/Vault.sol#L276)

Recommendation.

Do not shadow declarations, it’s dangerous to misuse variable/method.

Status.

NOT_ISSUE
ACKNOWLEDGED

26. Compilation-time const calculation

At

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/strategies/pancakeswap/PancakeMasterChefLPStrategy.sol#L26 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/strategies/pancakeswap/PancakeMasterChefLPStrategy.sol#L26)
  you can just write `bytes32(uint256(keccak256("eip1967.strategyStorage.poolId")) - 1))` instead of unclear hash.

The same for.

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/GovernableInit.sol#L9 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/GovernableInit.sol#L9)

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/upgradability/BaseUpgradeabilityProxy.sol#L24 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/upgradability/BaseUpgradeabilityProxy.sol#L24)

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/VaultStorage.sol#L7-19 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/VaultStorage.sol#L7-19)

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/upgradability/BaseProxyStorage.sol#L6-8 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/upgradability/BaseProxyStorage.sol#L6-8)

Recommendation.

Calculate const at compilation time using statement.

Status.

NOT_ISSUE
ACKNOWLEDGED

27. forward reward in 1 transfer instead of 2

At

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/strategies/pancakeswap/PancakeMasterChefLPStrategy.sol#L187 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/strategies/pancakeswap/PancakeMasterChefLPStrategy.sol#L187)

we first swap token to the contract address and then at

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/strategies/pancakeswap/PancakeMasterChefLPStrategy.sol#L317 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/strategies/pancakeswap/PancakeMasterChefLPStrategy.sol#L317)
- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/strategies/pancakeswap/PancakeMasterChefLPStrategy.sol#L99 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/strategies/pancakeswap/PancakeMasterChefLPStrategy.sol#L99)

we transfer it to vault / rewardPool

Recommendation.

Specify correct receiver of the tokens on behalf of the contract address.

Status.

NOT_ISSUE
ACKNOWLEDGED

28. revert in modifier

At

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/Migrations.sol#L12 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/Migrations.sol#L12)

the modifier should revert in else branch.

Recommendation.

Add revert.

Status.

NOT_ISSUE
ACKNOWLEDGED

29. `delete` is more exact than `new address[](0)`

At

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/strategies/pancakeswap/PancakeMasterChefLPStrategy.sol#L418-419 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/strategies/pancakeswap/PancakeMasterChefLPStrategy.sol#L418-419)
- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/strategies/pancakeswap/PancakeMasterChefLPStrategy.sol#L72-73 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/strategies/pancakeswap/PancakeMasterChefLPStrategy.sol#L72-73)
- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/strategies/pancakeswap/PancakeMasterChefLPStrategy.sol#L75 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/strategies/pancakeswap/PancakeMasterChefLPStrategy.sol#L75)

you can just write `delete pancakeswapRoutes[uniLPComponentToken1]`

Recommendation.

Use `delete` .

Status.

NOT_ISSUE
ACKNOWLEDGED

30. Unused methods

At

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/lib/Strings.sol#L5 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/lib/Strings.sol#L5)
  these methods are never used.

Moreover, in modern solidity versions there is embedded way to concatenate strings.

Recommendation.

Remove unused methods.

Status.

NOT_ISSUE
ACKNOWLEDGED

31. Replace as much code as possible with open-source popular alternatives.

At

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/GovernableInit.sol#L7 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/GovernableInit.sol#L7)

the contract functionality is very similar to https://github.com/OpenZeppelin/openzeppelin-contracts-upgradeable/blob/master/contracts/access/AccessControlUpgradeable.sol (https://github.com/OpenZeppelin/openzeppelin-contracts-upgradeable/blob/master/contracts/access/AccessControlUpgradeable.sol)

you should try to replace as much code with ready-to-use popular solutions. Much less space to make a mistake.

… the same for Controllable, Migrations, Vault …

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/Storage.sol (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/Storage.sol) could be replaced with openzeppelin Roles.

Recommendation.

Use ready-to-use popular contracts.

Status.

NOT_ISSUE
ACKNOWLEDGED

32. Contract should be abstract.

At

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/Controllable.sol#L5 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/Controllable.sol#L5)

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/LPTokenWrapper.sol#L7 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/LPTokenWrapper.sol#L7)

Recommendation.

Make contract `abstract`

Status.

NOT_ISSUE
ACKNOWLEDGED

33. Be careful with changing state after external calls.

At

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/LPTokenWrapper.sol#L44 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/LPTokenWrapper.sol#L44)
- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/NoMintRewardPool.sol#L162 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/NoMintRewardPool.sol#L162)

some states are changes after external calls. This is potentially dangerous for reentry attacks.

Recommendation.

Be careful for such places. Place state change before external calls.

Status.

NOT_ISSUE

34. Unused contract.

At

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/lib/CanTransferRole.sol (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/lib/CanTransferRole.sol) the contract is never used.

Recommendation.

Remove.

Status.

NOT_ISSUE

35. Override is not need

At

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/Controller.sol#L22 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/Controller.sol#L22)
- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/Controller.sol#L33 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/Controller.sol#L33)

why do we need `override` ?

Recommendation.

Remove.

Status.

NOT_ISSUE

36. Expensive work with storage

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/NotifyHelper.sol#L42 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/NotifyHelper.sol#L42)

Recommendation.

If you really care about gas I would recommend require sorted arg to be passed and check that address a[i+1] > a[i] uint160(address(msg.sender))

Status.

NEW

37. transfer ownership

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/RewardDistributionRecipient.sol#L20 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/RewardDistributionRecipient.sol#L20)
  can rewardDistributor do it? not only owner?

38. deprecated `msg.sender.transfer`

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/interfaces/WBNB.sol#L31 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/interfaces/WBNB.sol#L31)

Recommendation

Use `call` .
See https://solidity-by-example.org/sending-ether/ (https://solidity-by-example.org/sending-ether/)

39. require new strategy

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/interfaces/Vault.sol#L204 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/interfaces/Vault.sol#L204)

Recommendation

Use `require` instead of `if`

40. emit event on unexpected state

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/interfaces/Vault.sol#L240 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/interfaces/Vault.sol#L240)

Recommendation

Emit special event `UnexpectdState` for unexpected execution branches for easy smart-contract monitoring.

41. duplicated logic

- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/Vault.sol#L324 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/Vault.sol#L324)
- https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/upgradeability/BaseUpgradeableStrategy#L68 (https://github.com/VaultyFinance/contracts/blob/289b19252f150c13fa593c6add8563d383b5a17e/upgradeability/BaseUpgradeableStrategy#L68)

and also in NFT folder

the methods

- scheduleUpgrade
- shouldUpgrade
- finalizeUpgrade

are duplicated.

Recommendation

Create abstract parent class.