Vesper Pools

January 2022

coinspect

Vesper Pools

Smart Contract Audit

V220112

Prepared for Vesper • January 2022

1. Executive Summary

In **January 2022**, **Vesper** engaged Coinspect to perform a source code review of the latest update to **vesper-pools-v3**. The objective of the project was to continue to evaluate the security of the smart contracts.

The audit scope included changes to the pool contracts, new earn strategies, updates to EarnDrip, the new VSP BuyBack contract, changes in the curve and convex strategies along with the fix to a previously identified issue.

In **April 2022** Coinspect conducted a new review limited to the code modified to address the security issues identified during the initial assessment.

The following issues were identified during the initial assessment and their status has been updated on the latest review:

High Risk	Medium Risk	Low Risk
0	**0**	**1**
Fixed 0	Fixed 0	Fixed 1

2. Assessment and Scope

The audit started on **January 3, 2022** and was conducted on the Git repository at https://github.com/bloqpriv/vesper-pools-v3. The commit reviewed during this engagement was `9aaa264215a9b352f46261e956b4caa33e9ec168` from **December 21, 2021**.

The scope of the audit was limited to the latest version of the following Solidity source files, shown here with their sha256sum hash:

```
17b9dd0046758767e35f41abe264bdb1893377cb666fb0ed176d3cd15acc7c38  dependencies/openzeppelin/utils/structs/EnumerableSet.sol
ca5785b4bf93e62d5d27c86a2dc7550422e2a36cd92788c905824f0a58ffe101  dependencies/openzeppelin/utils/structs/README.md
a72a552c74171a5cf82c562c19f8155a20cc73deb20c77ab382fe293c848cb8b  interfaces/curve/IDeposit.sol
81f33bab939a954d87c4bfbe257aa24726efdd48ea6fa40eaab8fc0843f152d7  interfaces/curve/IDepositZap.sol
81674c559f4ee1a8c439229fd7726272014c8746b94724596dffae2e7a2a7123  interfaces/curve/ILiquidityGauge.sol
46a7454ae3f9e423af5d2f554a8635d5fd58e65abbeff24a6646cbd4e2429aea  interfaces/curve/IMetapoolFactory.sol
fd521c9b9feeb6ac5eb6b399dcd69ed1e54456b45169ee990a65ab6d62b79c5b  interfaces/curve/IStableSwap.sol
29a918f23d45d3b1b22f90fc7abc690c73f700bfe6eae792d9d3bdf47b30e3cd  interfaces/vesper/IPoolAccountant.sol
11621b391d4aee91b2fcb13bf98ac46eadc0b7167fbf2225381d551995d026ca  interfaces/vesper/IStrategy.sol
175d884b33c3b53e00f582bcdaf8e8ad1e28b3908e843eef9137092e80dee3da  interfaces/vesper/IVesperPool.sol
4ef4dfae45363ae3c61ec9db619576eed0e58229a53ae0ef47995772ce59c885  pool/PoolAccountant.sol
dd70d0c32b0b4f92cebc8db6e7612ad21ee7fd4398a2ac85c21e637a2e3f502f  pool/PoolRewards.sol
18033631116c400d0312c90565ae8145cae275588d75df9425eedf6e02b3fc5f  pool/PoolShareToken.sol
c0e4108c246703d8b1961b7067f2206205a1eac026837345355bcd63e07019ed  pool/PoolStorage.sol
6ab45be27b90d953ad0371d283bee197891a8879fe5b91ad5cad25e26737012c  pool/VETH.sol
22995d31ff8a29aea1b03efd450400d566033747dc9905e41f6bd020d1be153c  pool/VPool.sol
a3d09800178df6282ec3fc699af72d91954b9ffa4c65f94b9b3b26168cdd1215  pool/VPoolBase.sol
f4bf772b653675111fd56d3d94aaab932d7583d4d1f0aa3bb02cac918443a12f  pool/earn/VesperEarnDrip.sol
98f895daec8268426291d4ae47a50361c1020e13acc4ab85d5b72d212e090e3b  pool/vfr/VFRBuffer.sol
1f60795d694d48ca93730da2cac1638cb8051e795a3f650179cb5c2eb97c31c8  pool/vfr/VFRPool.sol
ae95ba4f98b764edccd7651bb5f75e1bc3089ebd7c1c66115102b95936a2afb4  pool/vfr/VFRStablePool.sol
bf3c3b333cdf7ce4dcd4c16473ec26aa87649c950574609636b9a6615c257e3e  strategies/Earn.sol
8bd3265e8ddc81c16bf9073865663a748efc85827e0c171160462027c476d999  strategies/Strategy.sol
44f8762ed3a11940b60f87fa490ee749257eef5b64da475c284d20491292fd69  strategies/aave/AaveCore.sol
f8e276ad776a777aebe95fa21be4d38ea9c2f0c14b51604b9fcdf484ae898e5f  strategies/aave/AaveStrategy.sol
8004a3c19000e40826bd86cc7d35e0b69f3919904698da8e577519138b7edd6a  strategies/aave/AaveStrategyAvalanche.sol
bb135ee417828efdf5d9abfdb3b72fe138f2044fae62a605afce48350edb7e4e  strategies/aave/AaveStrategyPolygon.sol
452ae8cd3548e3b511ebb2acae4cf8216a244c3019f2f1eee06eaa03fc9c3916  strategies/aave/AaveV1Strategy.sol
5ed4d959594299aee46f74df2e57b2c2527548d1c8085469be535f9bef9313ab  strategies/aave/earn/EarnAaveStrategy.sol
b03c251d9956571e74974f58c0beb024ff19b94b99a22eacffda05c03fdc1648  strategies/alpha/AlphaLendStrategy.sol
6db97dfb59d534860a30f177c2ce5385a67800ec47f7ada524e5babf21e69c22  strategies/alpha/AlphaLendStrategyETH.sol
6a395a2cd268d7ad3d550e17aafc3f4c4d10e37093b96250fa4a50d715f93efb  strategies/alpha/earn/EarnAlphaLendStrategy.sol
dcf3631b73307d14086fbec1f91dc05e74111529291b2b00f6fdd2f3d289de49  strategies/alpha/earn/EarnAlphaLendStrategyETH.sol
0ea46d7ac25f3c4d4f057413741bb2bc62c6e6f1e2bccabb1f46b28b1301666e  strategies/compound/CompoundLeverageStrategy.sol
1bd224262117c13dbe759b62e8d2eca7c88c80879563175d3393fd726af6c8b8  strategies/compound/CompoundLeverageStrategyETH.sol
ca95d9169a9d13649bb7ac2ae638ee9c982fd122e3def7ddf1a3283a90129369  strategies/compound/CompoundLeverageStrategyLINK.sol
09996580f5405891ccdb5571ebec75586632af5734defe1f29377b413bbfa694  strategies/compound/CompoundLeverageStrategyUNI.sol
638b429a5bcd6817ccb56d279ec1f9de2b657193f2ad7c75c6a13a1da7daf871  strategies/compound/CompoundStrategy.sol
a0d2a3fb095bc2ddf8d5d35a7ecb04820d8e2c1ae39f1de520c4c3f32b335418  strategies/compound/CompoundStrategyETH.sol
b6bedcab172dec7f3c99308f5c80ca5c3279001a8726a8ec1a76401811e71d55  strategies/compound/CompoundXYStrategyETH.sol
e39e3f34a99e23de87296af66956fa513985cf1b680ca92b10ffa24647cdd93d  strategies/compound/earn/EarnCompoundStrategy.sol
48fcf7d0bb8c6b880e800257404feea5ad9fd9bc3678b0394e1ea57cb52b5305  strategies/compound/earn/EarnCompoundStrategyETH.sol
a3412fefc95053a54f8820503bb8c0527c4c82dc833d19019e61ceaddbffa533  strategies/compound/vfr/CompoundCoverageStrategy.sol
cc315d2573accba6362af44ed22713c7514e41f99bc8a14cee4e3a864499e9cb  strategies/compound/vfr/CompoundStableStrategy.sol
03c26250de5d2a781752c891aa3dba26a3209a9c30199c2a08a07d54f1b38885  strategies/convex/2Pool/Convex2PoolStrategy.sol
e22bfc0e1c8d3f7243c4db2c9f4141344fd1fcbe7f7b1ae9af12f3e6f4163f1e  strategies/convex/2Pool/Convex2PoolStrategyMIMUSTPool.sol
897d6fe884f89dcfc75c8dea5f949fca2dd544eb050c4ce4f7c2cbea9b5aaa32  strategies/convex/4Pool/Convex4MetaPoolStrategy.sol
f42103d786dd2f5ee759b220d1db408de392dd4b3d65fb021a271053c8c8aaa7  strategies/convex/4Pool/Convex4MetaPoolStrategyMIMPool.sol
6582eaa0e7e523cf362b355c23d86a4a1c9cb2b12207bf28c6ee7cd1e5426af0  strategies/convex/4Pool/Convex4PoolStrategy.sol
76b0c39a6a0adc0bc0c1e886376dead7fcf811519825eaada064c473fd0dca5d  strategies/convex/4Pool/Convex4PoolStrategySUSDPool.sol
a8d6e2d670c13b246ebcab5a14c027fec0034a87e349fbf582600f37df999a3d  strategies/convex/Convex3PoolStrategy.sol
f66f92c87d0233c18fa4e440767a28a0d2092eb8cbeda20346a0808410776c49  strategies/convex/ConvexSBTCPoolStrategy.sol
59011cc7e6d2349d47fa603b4e638affdafa54897fe4ad522bdf8ba49e7f2263  strategies/convex/ConvexStrategy.sol
3b3c616eec0ccdcb21638553cf9ecbb1b19ce9c4542390aacd29cc62f6210579  strategies/convex/ConvexStrategyBase.sol
c1f72cef10e6a3981d08304741c4c564b896eee2af21c2f41cdb1b4107e9ef6a  strategies/convex/vfr/ConvexCoverage3PoolStrategy.sol
```

```
506ef88b49adaa1abc53f2a30c1d6026ed6ec01bc078dc4a7944b9ab0308e96e  strategies/convex/vfr/ConvexCoverageStrategy.sol
0d25e7051ec07c0fbd7ae6577732846d0722e42e052e91847d7898a8ff1cb75d  strategies/convex/vfr/ConvexStable3PoolStrategy.sol
fb1f646cdbc0abe10212a4c28cb02feb99e575a7d6fd339d789a2e647df12ea8  strategies/convex/vfr/ConvexStableStrategy.sol
6e7bf7ac0f8723bf063fe570e3b79b99f8eca8b03dc9b52e4aa6c94fdd3a726a  strategies/curve/2Pool/Crv2PoolStrategy.sol
e1827cd8df192e23cc304821bb80e70c2f445c02d8918b5ff77b27c2c18c597a  strategies/curve/2Pool/Crv2PoolStrategyArbitrumUSDCUSDTPool.sol
f1e6127d5a91f8583b49c03615ac348bc08315f9706cf22ed50c2558aded0945  strategies/curve/2Pool/Crv2PoolStrategyMIMUSTPool.sol
f057912ac26d721c53aaf08d004dbc93102a8c84003d82089d0d9c22342fcd30  strategies/curve/3Pool/Crv3PoolStrategy.sol
3b0d3430b6f093b0351ee5a7e9168e32674c90e4e5ea5b52182d7a20cb32818b  strategies/curve/3Pool/CrvSBTCPoolStrategy.sol
42138d2e6428b1ee0b319c5869773590cc7394603cf5c8f10f08d77f45a7b1fa  strategies/curve/3Pool/earn/EarnCrvSBTCPoolStrategy.sol
5b2dd5afee177b4e29e5389f21b853570a888dc58b8d1a0fc8bd7f8f34af36ce  strategies/curve/4Pool/Crv4MetaPoolStrategy.sol
d851fc601c2905f7daa01fef64e628a30cfc2b58265eff0fceb1164c3134be69  strategies/curve/4Pool/Crv4MetaPoolStrategyMIMPool.sol
c45e656697e04734231274a89edb1d39012d0291f11af0e837de704f7255b950  strategies/curve/4Pool/Crv4PoolStrategy.sol
5da61f83a1d583770669e4f3ba93401c66edd6bfc9c9df142130036dcf639636  strategies/curve/4Pool/Crv4PoolStrategySUSDPool.sol
005d45dfe285e5bb50065e53b7dfc2141293edebdaa905736133ba9c44397f1a  strategies/curve/CrvBase.sol
f5ca596f1a9533b078bcf66c346c53a4ff6419b215022c8e8ca0acb5d764ccac  strategies/curve/CrvPoolStrategyBase.sol
005ea0ccbf5540a63703d2ed1f98ba96aff9b3273e6b4d5276a9c76711a37f8e  strategies/curve/a3Pool/CrvA3PoolStrategy.sol
73731df84ed778b8a6c8212448ed59453749998205105cb4994d2ebac37fb2a6  strategies/maker/AaveMakerStrategy.sol
a00f0e7e9bfdcbd13957347f10ffb93c962b0a76b02a73dd40bcaac2a00f5d00  strategies/maker/CompoundMakerStrategy.sol
c29cc054605638a8808d627b1c3b0d22b0c1f3882e3cbb2412229e16794911f0  strategies/maker/MakerStrategy.sol
6173042096701d4a91733f59632929cdae264735b1cad6a5d5e290a5ce27bd38  strategies/maker/VesperMakerStrategy.sol
c8af05a2b6969a82bac06fcde96dded1a0e7787dcc374d587da8caf5cf85c581  strategies/maker/earn/EarnAaveMakerStrategy.sol
77d52a7f302aeec54cf82bb7ee4d0eab20e9a5840795ba49c300e94eda0414c8  strategies/maker/earn/EarnCompoundMakerStrategy.sol
8e18c2d216f231bc22548cfbbbfdad014c3f220a444d282ea2736063e0a0e156  strategies/maker/earn/EarnVesperMakerStrategy.sol
2bbe50b9d307e5a50ff756eb88eded9c76e67f56f20a350889c5b46a04b54b21  strategies/rari-fuse/RariFuseStrategy.sol
e4cf10ad7f87b54485db6c3153916b6fd1e33d40b86180abd8977b44ecda17a9  strategies/rari-fuse/RariFuseStrategyETH.sol
cb37bb219b91dc6b41edd38eaa123f8cac6dfe95ed581838a1ecee61a732d835  strategies/rari-fuse/earn/EarnRariFuseStrategy.sol
a3c52d10359db48af60a9ec269d65f276b72bc23f76de2b79370e35fc39ce1a2  strategies/rari-fuse/earn/EarnRariFuseStrategyETH.sol
f692321bd21a8d26825ad5970aec345bb82ea84c10ee3f9a78693bf2da692c99  strategies/vesper/VesperStrategy.sol
ae0325f097b288cddf9c6435d720257a05a429aa4b9e981198612470d446e2c0  strategies/vesper/earn/EarnVesperStrategy.sol
456685225816ebbdc085626051a823517e837dcf925777557e615075e2c0e95a  strategies/vesper/earn/EarnVesperStrategyVSPDrip.sol
5750ff152729ac85a0a9d08739e6be9310ee57840e44b0f60f3ce7a63d091799  strategies/vesper/vfr/VesperCoverageStrategy.sol
31646b6e6e5211d67d9b9ff4605551b4d7faab3388857ff0420ff92e6bb338e9  strategies/vesper/vfr/VesperStableStrategy.sol
bb72a9933eb707999bbf91890b6f745e69cdd13491323846452e99ead9d4aff5  strategies/yearn/YearnStrategy.sol
07d372fdb7b4d54179a8043bb29fe866f8fe9a3a050c326ff0d544a7e53ec7ed  strategies/yearn/earn/EarnYearnStrategy.sol
```

Pool changes

The pool modifications included replacing AddressList by the Open Zeppelin EnumerableSet implementation, a new external deposit fee, and updates to the deposit and withdrawal logic.

The variable externalDepositFee from the PoolAccountant contract is calculated based on externalDepositFee from each strategy, debtRatio, and totalDebtRatio. Thus, the main externalDepositFee of the pool must be updated every time any of these values is modified. One update that is missing is when the _reportLoss function is called through the reportEarning function (see VSP-44), here the totalDebt value of the strategy may change while leaving the externalDepositFee unchanged.

The VesperEarnDrip contract extends the PoolRewards contract for Earn pools, adding multiple token support for Earn strategies. There is a small inconsistency between the RewardPaid event emitted when claiming rewards and the reward listed when calling the claimable function. The claimable function returns the claimable amount of the growToken transformed into the dripToken, but the RewardPaid event emitted from the claimReward function in the PoolRewards contract displays the growToken amount. This can result in misunderstanding by users.

Changes in Curve and Convex strategies

The changes to the Curve and Convex strategies include support for 2Pool, 3Pool, 4Pool and 4MetaPool for Curve and Convex strategies.

Convex strategies have redundant code. Contracts such as Convex2PoolStrategy and its parent contract ConvexStrategyBase both perform the same swap of the CVX tokens to the _toToken provided. This has no impact on the security of the contracts, but repeated code makes future updates error-prone.

In the Curve strategies the _depositToCurve function is overridden. The only implementation that considers a slippage for the _minLpAmount and calls _calcAmtOutAfterSlippage is the one of Crv2PoolStrategy.

```
uint256 _minLpAmount = _calcAmtOutAfterSlippage(
            ((_amt * _getSafeUsdRate()) / crvPool.get_virtual_price()) * 10**(18 - coinDecimals[collIdx]),
            crvSlippage);
```

The other implementations (i.e. Crv4MetaPoolStrategy, Crv4PoolStrategy, and CrvA3PoolStrategy) calculate _minLpAmount differently. This is not directly exploitable, but may cause strategies to behave slightly differently. Coinspect recommends unifying the aforementioned behavior.

Updated strategies

Several Earn strategies were updated in the project including the strategies for Maker, Fuse, Alpha and Yearn.

The code was modified to allow new strategies to be deployed without compiling a new version of the code if only the name and tokenAddress values change.

Additional changes

`BuyBack` is a new utility contract that exposes functions for reinvesting in `VSP` provided a given asset. The exposed functions are correct, but the contract itself is not used by other contracts.

An issue where the wrong amount was being withdrawn from the `AlphaLendStrategy` was solved by adding the `alpha` amount to the `safeBox` amount when calculating the `totalValue`.

3. Summary of Findings

Id	Title	Total Risk	Fixed
VSP-44	Incorrect external deposit fee	Low	✔
VSP-45	Unnecessary gas expenditure	Info	✘

4. Detailed Findings

VSP-44 Incorrect external deposit fee

Total Risk
Low

Impact
Low

Location
`pool/PoolAccountant.sol`

Fixed
✔

Likelihood
Low

Description

The `externalDepositFee` value can be obsolete when the `_reportLoss` function is called.

The `externalDepositFee` is a value that depends on the configuration and current state of the strategies, as seen in the `_recalculatePoolExternalDepositFee` function:

```
function _recalculatePoolExternalDepositFee() internal {
    uint256 _len = strategies.length;
    uint256 _externalDepositFee;

    // calculate poolExternalDepositFee and weightedFee for each strategy
    if (totalDebtRatio != 0) {
        for (uint256 i = 0; i < _len; i++) {
            _externalDepositFee += (strategy[strategies[i]].externalDepositFee *
strategy[strategies[i]].debtRatio) / totalDebtRatio;
        }
    }

    // Update externalDepositFee and emit event
    emit UpdatedPoolExternalDepositFee(externalDepositFee, externalDepositFee = _externalDeposi
}
```

The consequence is that when any of these values is updated, the `externalDepositFee` must be recalculated.

For instance, when the `_reportLoss` function is called the `externalDepositFee` variable is not recalculated, but the `debtRatio` variable is updated.

```
function _reportLoss(address _strategy, uint256 _loss) internal {
    uint256 _currentDebt = strategy[_strategy].totalDebt;
    require(_currentDebt >= _loss, Errors.LOSS_TOO_HIGH);
    strategy[_strategy].totalLoss += _loss;
    strategy[_strategy].totalDebt -= _loss;
    totalDebt -= _loss;
    uint256 _deltaDebtRatio = _min((_loss * MAX_BPS) / IVesperPool(pool).totalValue(),
strategy[_strategy].debtRatio);
    strategy[_strategy].debtRatio -= _deltaDebtRatio;
    totalDebtRatio -= _deltaDebtRatio;
}
```

Recommendation

Update the `externalDepositFee` variable when needed.

Status

April 20, 2022: Fixed in two steps

1. Added the `recalculatePoolExternalDepositFee` function that updates the value in commit `042117cc92fc5f6f3eb75ff71558148ca1a260dc`.
2. The fees are being replaced by the universal fee.

VSP-45 Unnecessary gas expenditure

Total Risk	Impact	Location
Info	-	`contracts/pool/PoolAccountant.sol`
Fixed ✘	Likelihood -	

Description

The `removeStrategy` function seeks through all the strategies before removing the correct one:

```
address[] memory _withdrawQueue = new address[](strategies.length);
uint256 j;
// After above update, withdrawQueue.length > strategies.length
for (uint256 i = 0; i < withdrawQueue.length; i++) {
    if (withdrawQueue[i] != _strategy) {
        _withdrawQueue[j] = withdrawQueue[i];
        j++;
    }
}
```

Recommendation

Provide an additional parameter with the index of the strategy to be removed.

Status

April 20, 2022: The Vesper team decided to keep the current code because the order of the elements must be preserved.

5. Disclaimer

The information presented in this document is provided "as is" and without warranty. The present security audit does not cover any off-chain systems or frontends that communicate with the contracts, nor the general operational security of the organization that developed the code.