SHERLOCK

SHERLOCK SECURITY REVIEW FOR

Prepared for: Blueberry
Prepared by: Sherlock
Lead Security Expert: obront
Dates Audited: February 6 - February 20, 2023
Prepared on: March 29, 2023

Introduction

Blueberry unifies the DeFi experience: Aggregating, Automating, and Boosting Capital Efficiency for top DeFi Strategies.

Scope

Github

```
Includes:
    - All contracts in `/contracts`
```

Findings

Each issue has an assigned severity:

- Medium issues are security vulnerabilities that may not be directly exploitable or may require certain conditions in order to be exploited. All major issues should be addressed.
- High issues are directly exploitable security vulnerabilities that need to be fixed.

Issues found

Medium	High
18	10

Issues not fixed or acknowledged

Medium	High
0	0

Security experts who found valid issues

obront
0x52
rvierdiiev
berndartmueller
Jeiwan
cducrest-brainbot
koxuan
rbserver
chaduke
carrot
Robert
evan
cergyk
tives
Ruhum
csanuragjain
y1cunhui
8olidity

minhtrng
XKET
Nyx
ctf_sec
Ch_301
sinarette
banditx0x
psy4n0n
sakshamguruji
peanuts
SPYBOY
Saeedalipoor01988
0xChinedu
Bauer
stent
0Kage
saian
Dug
Avci
Breeje
GimelSec
tsvetanovv
WatchDogs
HonorLt
Aymen0909
Chinmay
hl_

Issue H-1: Too few ICHI v2 farming reward tokens transferred to the user due to incorrect decimal precision

Source: https://github.com/sherlock-audit/2023-02-blueberry-judging/issues/319

Found by

berndartmueller, 0x52

Summary

The `burn` function in the `WIchiFarm` contract transfers too few `ICHI` **v2** farming reward tokens to the caller due to using 9 decimals instead of 18 decimals for the `ICHI` **v2** token.

Vulnerability Detail

Closing an ICHI vault spell farming position burns the wrapped ICHI vault LP tokens (`WIchiFarm` ERC-1155 tokens). Farming rewards are harvested from the ICHI farm (see contract on Etherscan) and received as `ICHI` **v1** tokens.

The `ICHI` **v1** ERC-20 token uses **9 decimals** (see token on Etherscan), whereas the `ICHI` **v2** ERC-20 token uses **18 decimals** (see token on Etherscan).

Those received `ICHI` **v1** tokens are then converted to **v2** tokens in line 134.

To calculate the user's share of eligible `ICHI` **v2** reward tokens, the reward per share accumulator `stIchiPerShare` at the time of minting the `WIchiFarm` token and the current `enIchiPerShare` accumulator is used.

However, those accumulator values are in **9 decimals** precision (please see the `ichiFarmV2.harvest` function for proof that `pool.accIchiPerShare` uses 9 decimals, otherwise the `ICHI` token transfer would fail due to inflated `_pendingIchi`). Given that `amount` is in **18 decimals**, the calculation of `stIchi` and `enIchi` in lines 143 and 144 will result in a value with **9 decimals** precision.

As previously mentioned, the `ICHI` **v2** token uses **18 decimals**. Therefore, too few `ICHI` **v2** tokens are transferred.

Impact

Users will receive substantially fewer `ICHI` v2 farming reward tokens than expected.

Code Snippet

wrapper/WIchiFarm.sol#L143-L144

```
116: function burn(uint256 id, uint256 amount)
117:     external
118:     nonReentrant
119:     returns (uint256)
120: {
121:     if (amount == type(uint256).max) {
122:         amount = balanceOf(msg.sender, id);
123:     }
124:     (uint256 pid, uint256 stIchiPerShare) = decodeId(id);
125:     _burn(msg.sender, id, amount);
126:
127:     uint256 ichiRewards = ichiFarm.pendingIchi(pid, address(this));
128:     ichiFarm.harvest(pid, address(this));
129:     ichiFarm.withdraw(pid, amount, address(this));
130:
131:     // Convert Legacy ICHI to ICHI v2
132:     if (ichiRewards > 0) {
133:         ICHIv1.safeApprove(address(ICHI), ichiRewards);
134:         ICHI.convertToV2(ichiRewards);
135:     }
136:
137:     // Transfer LP Tokens
138:     address lpToken = ichiFarm.lpToken(pid);
139:     IERC20Upgradeable(lpToken).safeTransfer(msg.sender, amount);
140:
141:     // Transfer Reward Tokens
142:     (uint256 enIchiPerShare, , ) = ichiFarm.poolInfo(pid);
143:     uint256 stIchi = (stIchiPerShare * amount).divCeil(1e18);
144:     uint256 enIchi = (enIchiPerShare * amount) / 1e18; // @audit-info
↪  `enIchi` and `stIchi` are in 9 decimal precision
145:
146:     if (enIchi > stIchi) {
147:         ICHI.safeTransfer(msg.sender, enIchi - stIchi);
148:     }
149:     return pid;
150: }
```

Tool used

Manual Review

Recommendation

Consider changing the denominator in lines 143 and 144 from `1e18` to `1e9` to use the required `18` decimals for the `ICHI` v2 token.

Issue H-2: Users who deposit extra funds into their Ichi farming positions will lose all their ICHI rewards

Source: https://github.com/sherlock-audit/2023-02-blueberry-judging/issues/158

Found by

carrot, rvierdiiev, minhtrng, obront, sinarette, tives, berndartmueller, 0x52

Summary

When a user deposits extra funds into their Ichi farming position using `openPositionFarm()`, the old farming position will be closed down and a new one will be opened. Part of this process is that their ICHI rewards will be sent to the `IchiVaultSpell.sol` contract, but they will not be distributed. They will sit in the contract until the next user (or MEV bot) calls `closePositionFarm()`, at which point they will be stolen by that user.

Vulnerability Detail

When Ichi farming positions are opened via the `IchiVaultSpell.sol` contract, `openPositionFarm()` is called. It goes through the usual deposit function, but rather than staking the LP tokens directly, it calls `wIchiFarm.mint()`. This function deposits the token into the `ichiFarm`, encodes the deposit as an ERC1155, and sends that token back to the Spell:

```
function mint(uint256 pid, uint256 amount)
    external
    nonReentrant
    returns (uint256)
{
    address lpToken = ichiFarm.lpToken(pid);
    IERC20Upgradeable(lpToken).safeTransferFrom(
        msg.sender,
        address(this),
        amount
    );
    if (
        IERC20Upgradeable(lpToken).allowance(
            address(this),
            address(ichiFarm)
        ) != type(uint256).max
    ) {
        // We only need to do this once per pool, as LP token's allowance won't
↪   decrease if it's -1.
        IERC20Upgradeable(lpToken).safeApprove(
```

```
            address(ichiFarm),
            type(uint256).max
        );
    }
    ichiFarm.deposit(pid, amount, address(this));
    // @ok if accIchiPerShare is always changing, so how does this work?
    // it's basically just saving the accIchiPerShare at staking time, so when
↪   you unstake, it can calculate the difference
    // really fucking smart actually
    (uint256 ichiPerShare, , ) = ichiFarm.poolInfo(pid);
    uint256 id = encodeId(pid, ichiPerShare);
    _mint(msg.sender, id, amount, "");
    return id;
}
```

The resulting ERC1155 is posted as collateral in the Blueberry Bank.

If the user decides to add more funds to this position, they simply call `openPositionFarm()` again. The function has logic to check if there is already existing collateral of this LP token in the Blueberry Bank. If there is, it removes the collateral and calls `wIchiFarm.burn()` (which harvests the Ichi rewards and withdraws the LP tokens) before repeating the deposit process.

```
function burn(uint256 id, uint256 amount)
    external
    nonReentrant
    returns (uint256)
{
    if (amount == type(uint256).max) {
        amount = balanceOf(msg.sender, id);
    }
    (uint256 pid, uint256 stIchiPerShare) = decodeId(id);
    _burn(msg.sender, id, amount);

    uint256 ichiRewards = ichiFarm.pendingIchi(pid, address(this));
    ichiFarm.harvest(pid, address(this));
    ichiFarm.withdraw(pid, amount, address(this));

    // Convert Legacy ICHI to ICHI v2
    if (ichiRewards > 0) {
        ICHIv1.safeApprove(address(ICHI), ichiRewards);
        ICHI.convertToV2(ichiRewards);
    }

    // Transfer LP Tokens
    address lpToken = ichiFarm.lpToken(pid);
    IERC20Upgradeable(lpToken).safeTransfer(msg.sender, amount);
```

```
    // Transfer Reward Tokens
    (uint256 enIchiPerShare, , ) = ichiFarm.poolInfo(pid);
    uint256 stIchi = (stIchiPerShare * amount).divCeil(1e18);
    uint256 enIchi = (enIchiPerShare * amount) / 1e18;

    if (enIchi > stIchi) {
        ICHI.safeTransfer(msg.sender, enIchi - stIchi);
    }
    return pid;
}
```

However, this deposit process has no logic for distributing the ICHI rewards. Therefore, these rewards will remain sitting in the `IchiVaultSpell.sol` contract and will not reach the user.

For an example of how this is handled properly, we can look at the opposite function, `closePositionFarm()`. In this case, the same `wIchiFarm.burn()` function is called. But in this case, it's followed up with an explicit call to withdraw the ICHI from the contract to the user.

```
doRefund(ICHI);
```

This `doRefund()` function refunds the contract's full balance of ICHI to the `msg.sender`, so the result is that the next user to call `closePositionFarm()` will steal the ICHI tokens from the original user who added to their farming position.

Impact

Users who farm their Ichi LP tokens for ICHI rewards can permanently lose their rewards.

Code Snippet

https://github.com/sherlock-audit/2023-02-blueberry/blob/main/contracts/spell/IchiVaultSpell.sol#L199-L249

https://github.com/sherlock-audit/2023-02-blueberry/blob/main/contracts/wrapper/WIchiFarm.sol#L116-L150

Here is a link to the `harvest()` function on the IchiFarmV2.sol contract, which is called by `wIchiFarm.sol` and contains the logic for distributing ICHI rewards: https://github.com/ichifarm/ichi-farming/blob/206c44b790fbb2a1e3a655685eb3ab8d793c9f00/contracts/ichiFarmV2.sol#L238-L257

Tool used

Manual Review

Recommendation

In the `openPositionFarm()` function, in the section that deals with withdrawing existing collateral, add a line that claims the ICHI rewards for the calling user.

```
if (collSize > 0) {
    (uint256 decodedPid, ) = wIchiFarm.decodeId(collId);
    if (farmingPid != decodedPid) revert INCORRECT_PID(farmingPid);
    if (posCollToken != address(wIchiFarm))
        revert INCORRECT_COLTOKEN(posCollToken);
    bank.takeCollateral(collSize);
    wIchiFarm.burn(collId, collSize);
+   doRefund(ICHI);
}
```

Issue H-3: LP tokens are not sent back to withdrawing user

Source: https://github.com/sherlock-audit/2023-02-blueberry-judging/issues/151

Found by

rvierdiiev, minhtrng, Dug, Jeiwan, obront, chaduke, koxuan, sinarette, Ch_301, cergyk, evan, berndartmueller, 0x52, Bauer

Summary

When users withdraw their assets from `IchiVaultSpell.sol`, the function unwinds their position and sends them back their assets, but it never sends them back the amount they requested to withdraw, leaving the tokens stuck in the Spell contract.

Vulnerability Detail

When a user withdraws from `IchiVaultSpell.sol`, they either call `closePosition()` or `closePositionFarm()`, both of which make an internal call to `withdrawInternal()`.

The following arguments are passed to the function:

- strategyId: an index into the `strategies` array, which specifies the Ichi vault in question
- collToken: the underlying token, which is withdrawn from Compound
- amountShareWithdraw: the number of underlying tokens to withdraw from Compound
- borrowToken: the token that was borrowed from Compound to create the position, one of the underlying tokens of the vault
- amountRepay: the amount of the borrow token to repay to Compound
- amountLpWithdraw: the amount of the LP token to withdraw, rather than trade back into borrow tokens

In order to accomplish these goals, the contract does the following...

1) Removes the LP tokens from the ERC1155 holding them for collateral.

```
doTakeCollateral(strategies[strategyId].vault, lpTakeAmt);
```

2) Calculates the number of LP tokens to withdraw from the vault.

```
uint256 amtLPToRemove = vault.balanceOf(address(this)) - amountLpWithdraw;
vault.withdraw(amtLPToRemove, address(this));
```

3) Converts the non-borrowed token that was withdrawn in the borrowed token (not copying the code in, as it's not relevant to this issue).
4) Withdraw the underlying token from Compound.

```
doWithdraw(collToken, amountShareWithdraw);
```

5) Pay back the borrowed token to Compound.

```
doRepay(borrowToken, amountRepay);
```

6) Validate that this situation does not put us above the maxLTV for our loans.

```
_validateMaxLTV(strategyId);
```

7) Sends the remaining borrow token that weren't paid back and withdrawn underlying tokens to the user.

```
doRefund(borrowToken);
doRefund(collToken);
```

Crucially, the step of sending the remaining LP tokens to the user is skipped, even though the function specifically does the calculations to ensure that `amountLpWithdraw` is held back from being taken out of the vault.

Impact

Users who close their positions and choose to keep LP tokens (rather than unwinding the position for the constituent tokens) will have their LP tokens stuck permanently in the IchiVaultSpell contract.

Code Snippet

https://github.com/sherlock-audit/2023-02-blueberry/blob/main/contracts/spell/IchiVaultSpell.sol#L276-L330

Tool used

Manual Review

Recommendation

Add an additional line to the `withdrawInternal()` function to refund all LP tokens as well:

```
  doRefund(borrowToken);
  doRefund(collToken);
+ doRefund(address(vault));
```

Discussion

Gornutz

duplicate of 34

Issue H-4: Fail to accrue interests on multiple token positions

Source: https://github.com/sherlock-audit/2023-02-blueberry-judging/issues/140

Found by

cducrest-brainbot, rvierdiiev, Jeiwan

Summary

In `BlueBerryBank.sol` the functions `borrow`, `repay`, `lend`, or `withdrawLend` call `poke(token)` to trigger interest accrual on concerned token, but fail to do so for other token debts of the concerned position. This could lead to wrong calculation of position's debt and whether the position is liquidatable.

Vulnerability Detail

Whether a position is liquidatable or not is checked at the end of the `execute` function, the execution should revert if the position is liquidatable.

The calculation of whether a position is liquidatable takes into account all the different debt tokens within the position. However, the debt accrual has been triggered only for one of these tokens, the one concerned by the executed action. For other tokens, the value of `bank.totalDebt` will be lower than what it should be. This results in the debt value of the position being lower than what it should be and a position seen as not liquidatable while it should be liquidatable.

Impact

Users may be able to operate on their position leading them in a virtually liquidatable state while not reverting as interests were not applied. This will worsen the debt situation of the bank and lead to overall more liquidatable positions.

Code Snippet

execute checking isLiquidatable without triggering interests:

https://github.com/sherlock-audit/2023-02-blueberry/blob/main/contracts/BlueBerryBank.sol#L607

actions only poke one token (here for borrow):

https://github.com/sherlock-audit/2023-02-blueberry/blob/main/contracts/BlueBerryBank.sol#L709-L715

bank.totalDebt is used to calculate a position's debt while looping over every tokens:

https://github.com/sherlock-audit/2023-02-blueberry/blob/main/contracts/BlueBerryBank.sol#L451-L475

The position's debt is used to calculate the risk:

https://github.com/sherlock-audit/2023-02-blueberry/blob/main/contracts/BlueBerryBank.sol#L477-L495

The risk is used to calculate whether a debt is liquidatable:

https://github.com/sherlock-audit/2023-02-blueberry/blob/main/contracts/BlueBerryBank.sol#L497-L505

Tool used

Manual Review

Recommendation

Review how token interests are triggered. Probably need to accrue interests on every debt token of a position at the beginning of execute.

Issue H-5: Users can get around MaxLTV because of lack of strategyId validation

Source: https://github.com/sherlock-audit/2023-02-blueberry-judging/issues/129

Found by

8olidity, carrot, Jeiwan, obront, Ch_301, cergyk, rbserver

Summary

When a user withdraws some of their underlying token, there is a check to ensure they still meet the Max LTV requirements. However, they are able to arbitrarily enter any `strategyId` that they would like for this check, which could allow them to exceed the LTV for their real strategy while passing the approval.

Vulnerability Detail

When a user calls `IchiVaultSpell.sol#reducePosition()`, it removes some of their underlying token from the vault, increasing the LTV of any loans they have taken.

As a result, the `_validateMaxLTV(strategyId)` function is called to ensure they remain compliant with their strategy's specified LTV:

```
function _validateMaxLTV(uint256 strategyId) internal view {
    uint256 debtValue = bank.getDebtValue(bank.POSITION_ID());
    (, address collToken, uint256 collAmount, , , , , ) = bank
        .getCurrentPositionInfo();
    uint256 collPrice = bank.oracle().getPrice(collToken);
    uint256 collValue = (collPrice * collAmount) /
        10**IERC20Metadata(collToken).decimals();

    if (
        debtValue >
        (collValue * maxLTV[strategyId][collToken]) / DENOMINATOR
    ) revert EXCEED_MAX_LTV();
}
```

To summarize, this check:

- Pulls the position's total debt value
- Pulls the position's total value of underlying tokens
- Pulls the specified maxLTV for this strategyId and underlying token combination

- Ensures that `underlyingTokenValue * maxLTV > debtValue`

But there is no check to ensure that this `strategyId` value corresponds to the strategy the user is actually invested in, as we can see the `reducePosition()` function:

```
function reducePosition(
    uint256 strategyId,
    address collToken,
    uint256 collAmount
) external {
    doWithdraw(collToken, collAmount);
    doRefund(collToken);
    _validateMaxLTV(strategyId);
}
```

Here is a quick proof of concept to explain the risk:

- Let's say a user deposits 1000 DAI as their underlying collateral.
- They are using a risky strategy (let's call it strategy 911) which requires a maxLTV of 2X (ie `maxLTV[911][DAI] = 2e5`)
- There is another safer strategy (let's call it strategy 411) which has a maxLTV of 5X (ie `maxLTV[411][DAI] = 4e5`)
- The user takes the max loan from the risky strategy, borrowing $2000 USD of value.
- They are not allowed to take any more loans from that strategy, or remove any of their collateral.
- Then, they call `reducePosition()`, withdrawing 1600 DAI and entering `411` as the strategyId.
- The `_validateMaxLTV` check will happen on `strategyId = 411`, and will pass, but the result will be that the user now has only 400 DAI of underlying collateral protecting $2000 USD worth of the risky strategy, violating the LTV.

Impact

Users can get around the specific LTVs and create significantly higher leverage bets than the protocol has allowed. This could cause the protocol to get underwater, as the high leverage combined with risky assets could lead to dramatic price swings without adequate time for the liquidation mechanism to successfully protect solvency.

Code Snippet

https://github.com/sherlock-audit/2023-02-blueberry/blob/main/contracts/spell/IchiVaultSpell.sol#L266-L274

https://github.com/sherlock-audit/2023-02-blueberry/blob/main/contracts/spell/IchiVaultSpell.sol#L101-L113

Tool used

Manual Review

Recommendation

Since the collateral a position holds will always be the vault token of the strategy they have used, you can validate the `strategyId` against the user's collateral, as follows:

```
address positionCollToken = bank.positions(bank.POSITION_ID()).collToken;
address positionCollId = bank.positions(bank.POSITION_ID()).collId;
address unwrappedCollToken =
↪   IERC20Wrapper(positionCollToken).getUnderlyingToken(positionCollId);
require(strategies[strategyId].vault == unwrappedCollToken, "wrong strategy");
```

Issue H-6: Liquidator can take all collateral and underlying tokens for a fraction of the correct price

Source: https://github.com/sherlock-audit/2023-02-blueberry-judging/issues/127

Found by

cducrest-brainbot, rvierdiiev, obront, evan, berndartmueller, 0x52, XKET

Summary

When performing liquidation calculations, we use the proportion of the individual token's debt they pay off to calculate the proportion of the liquidated user's collateral and underlying tokens to send to them. In the event that the user has multiple types of debt, the liquidator will be dramatically overpaid.

Vulnerability Detail

When a position's risk rating falls below the underlying token's liquidation threshold, the position becomes liquidatable. At this point, anyone can call `liquidate()` and pay back a share of their debt, and receive a propotionate share of their underlying assets.

This is calculated as follows:

```
uint256 oldShare = pos.debtShareOf[debtToken];
(uint256 amountPaid, uint256 share) = repayInternal(
    positionId,
    debtToken,
    amountCall
);

uint256 liqSize = (pos.collateralSize * share) / oldShare;
uint256 uTokenSize = (pos.underlyingAmount * share) / oldShare;
uint256 uVaultShare = (pos.underlyingVaultShare * share) / oldShare;

pos.collateralSize -= liqSize;
pos.underlyingAmount -= uTokenSize;
pos.underlyingVaultShare -= uVaultShare;

// ...transfer liqSize wrapped LP Tokens and uVaultShare underlying vault shares
↪  to the liquidator
}
```

To summarize:

- The liquidator inputs a debtToken to pay off and an amount to pay
- We check the amount of debt shares the position has on that debtToken
- We call `repayInternal()`, which pays off the position and returns the amount paid and number of shares paid off
- We then calculate the proportion of collateral and underlying tokens to give the liquidator
- We adjust the liquidated position's balances, and send the funds to the liquidator

The problem comes in the calculations. The amount paid to the liquidator is calculated as:

```
uint256 liqSize = (pos.collateralSize * share) / oldShare
uint256 uTokenSize = (pos.underlyingAmount * share) / oldShare;
uint256 uVaultShare = (pos.underlyingVaultShare * share) / oldShare;
```

These calculations are taking the total size of the collateral or underlying token. They are then multiplying it by `share / oldShare`. But `share / oldShare` is just the proportion of that one type of debt that was paid off, not of the user's entire debt pool.

Let's walk through a specific scenario of how this might be exploited:

- User deposits 1mm DAI (underlying) and uses it to borrow $950k of ETH and $50k worth of ICHI (11.8k ICHI)
- Both assets are deposited into the ETH-ICHI pool, yielding the same collateral token
- Both prices crash down by 25% so the position is now liquidatable (worth $750k)
- A liquidator pays back the full ICHI position, and the calculations above yield `pos.collateralSize * 11.8k / 11.8k` (same calculation for the other two formulas)
- The result is that for 11.8k ICHI (worth $37.5k after the price crash), the liquidator got all the DAI (value $1mm) and LP tokens (value $750k)

Impact

If a position with multiple borrows goes into liquidation, the liquidator can pay off the smallest token (guaranteed to be less than half the total value) to take the full position, stealing funds from innocent users.

Code Snippet

https://github.com/sherlock-audit/2023-02-blueberry/blob/main/contracts/BlueBerryBank.sol#L511-L572

https://github.com/sherlock-audit/2023-02-blueberry/blob/main/contracts/BlueBerryBank.sol#L760-L787

Tool used

Manual Review

Recommendation

Adjust these calculations to use `amountPaid / getDebtValue(positionId)`, which is accurately calculate the proportion of the total debt paid off.

Issue H-7: Users can be liquidated prematurely because calculation understates value of underlying position

Source: https://github.com/sherlock-audit/2023-02-blueberry-judging/issues/126

Found by

obront

Summary

When the value of the underlying asset is calculated in `getPositionRisk()`, it uses the `underlyingAmount`, which is the amount of tokens initially deposited, without any adjustment for the interest earned. This can result in users being liquidated early, because the system undervalues their assets.

Vulnerability Detail

A position is considered liquidatable if it meets the following criteria:

```
((borrowsValue - collateralValue) / underlyingValue) >= underlyingLiqThreshold
```

The value of the underlying tokens is a major factor in this calculation. However, the calculation of the underlying value is performed with the following function call:

```
uint256 cv = oracle.getUnderlyingValue(
    pos.underlyingToken,
    pos.underlyingAmount
);
```

If we trace it back, we can see that `pos.underlyingAmount` is set when `lend()` is called (ie when underlying assets are deposited). This is the only place in the code where this value is moved upward, and it is only increased by the amount deposited. It is never moved up to account for the interest payments made on the deposit, which can materially change the value.

Impact

Users can be liquidated prematurely because the value of their underlying assets are calculated incorrectly.

Code Snippet

https://github.com/sherlock-audit/2023-02-blueberry/blob/main/contracts/BlueBerryBank.sol#L485-L488

https://github.com/sherlock-audit/2023-02-blueberry/blob/main/contracts/oracle/CoreOracle.sol#L182-L189

https://github.com/sherlock-audit/2023-02-blueberry/blob/main/contracts/BlueBerryBank.sol#L644

Tool used

Manual Review

Recommendation

Value of the underlying assets should be derived from the vault shares and value, rather than being stored directly.

Issue H-8: Interest component of underlying amount is not withdrawable using the `withdrawLend` function. Such amount is permanently locked in the BlueBerryBank contract

Source: https://github.com/sherlock-audit/2023-02-blueberry-judging/issues/109

Found by

berndartmueller, carrot, minhtrng, 0Kage, Jeiwan, chaduke, koxuan, Ruhum, cergyk, rbserver, stent, saian, XKET, GimelSec

Summary

Soft vault shares are issued against interest bearing tokens issued by `Compound` protocol in exchange for underlying deposits. However, `withdrawLend` function caps the withdrawable amount to initial underlying deposited by user (`pos.underlyingAmount`). Capping underlying amount to initial underlying deposited would mean that a user can burn all his vault shares in `withdrawLend` function and only receive original underlying deposited.

Interest accrued component received from Soft vault (that rightfully belongs to the user) is no longer retrievable because the underlying vault shares are already burnt. Loss to the users is permanent as such interest amount sits permanently locked in Blueberry bank.

Vulnerability Detail

withdrawLend function in BlueBerryBank allows users to withdraw underlying amount from `Hard` or `Soft` vaults. `Soft` vault shares are backed by interest bearing `cTokens` issued by Compound Protocol

User can request underlying by specifying `shareAmount`. When user tries to send the maximum `shareAmount` to withdraw all the lent amount, notice that the amount withdrawable is limited to the `pos.underlyingAmount` (original deposit made by the user).

While this is the case, notice also that the full `shareAmount` is deducted from `underlyingVaultShare`. User cannot recover remaining funds because in the next call, user doesn't have any vault shares against his address. Interest accrued component on the underlying that was returned by `SoftVault` to `BlueberryBank` never makes it back to the original lender.

```
wAmount = wAmount > pos.underlyingAmount
        ? pos.underlyingAmount
```

```
        : wAmount;

    pos.underlyingVaultShare -= shareAmount;
    pos.underlyingAmount -= wAmount;
    bank.totalLend -= wAmount;
```

Impact

Every time, user withdraws underlying from a Soft vault, interest component gets trapped in BlueBerry contract. Here is a scenario.

- Alice deposits 1000 USDC into `SoftVault` using the `lend` function of BlueberryBank at T=0
- USDC soft vault mints 1000 shares to Blueberry bank
- USDC soft vault deposits 1000 USDC into Compound & receives 1000 cUSDC
- Alice at T=60 days requests withdrawal against 1000 Soft vault shares
- Soft Vault burns 1000 soft vault shares and requests withdrawal from Compound against 1000 cTokens
- Soft vault receives 1050 USDC (50 USDC interest) and sends this to BlueberryBank
- Blueberry Bank caps the withdrawal amount to 1000 (original deposit)
- Blueberry Bank deducts 0.5% withdrawal fees and deposits 995 USDC back to user

In the whole process, Alice has lost access to 50 USDC.

Code Snippet

https://github.com/sherlock-audit/2023-02-blueberry/blob/main/contracts/BlueBerryBank.sol#L693

Tool used

Manual Review

Recommendation

Introduced a new variable to adjust positions & removed cap on withdraw amount.

Highlighted changes I recommend to withdrawLend with //******//.

```
function withdrawLend(address token, uint256 shareAmount)
        external
```

```
        override
        inExec
        poke(token)
    {
        Position storage pos = positions[POSITION_ID];
        Bank storage bank = banks[token];
        if (token != pos.underlyingToken) revert INVALID_UTOKEN(token);

        //*********-audit cap shareAmount to maximum value,
↪   pos.underlyingVaultShare*******
        if (shareAmount > pos.underlyingVaultShare) {
            shareAmount = pos.underlyingVaultShare;
        }

        // if (shareAmount == type(uint256).max) {
        //     shareAmount = pos.underlyingVaultShare;
        // }

        uint256 wAmount;
        uint256 amountToOffset; //*********- audit added this to adjust
↪   position********
        if (address(ISoftVault(bank.softVault).uToken()) == token) {
            ISoftVault(bank.softVault).approve(
                bank.softVault,
                type(uint256).max
            );
            wAmount = ISoftVault(bank.softVault).withdraw(shareAmount);
        } else {
            wAmount = IHardVault(bank.hardVault).withdraw(token, shareAmount);
        }

        //*********- audit calculate amountToOffset********
        //*********-audit not capping wAmount anymore*******
        amountToOffset = wAmount > pos.underlyingAmount
            ? pos.underlyingAmount
            : wAmount;

        pos.underlyingVaultShare -= shareAmount;
     //*********-audit subtract amountToOffset instead of wAmount*******
        pos.underlyingAmount -= amountToOffset;
        bank.totalLend -= amountToOffset;

        wAmount = doCutWithdrawFee(token, wAmount);

        IERC20Upgradeable(token).safeTransfer(msg.sender, wAmount);
    }
```

Issue H-9: BlueBerryBank#withdrawLend will cause underlying token accounting error if soft/hard vault has withdraw fee

Source: https://github.com/sherlock-audit/2023-02-blueberry-judging/issues/33

Found by

y1cunhui, rvierdiiev, csanuragjain, Ruhum, evan, 0x52

Summary

Soft/hard vaults can have a withdraw fee. This takes a certain percentage from the user when they withdraw. The way that the token accounting works in BlueBerryBank#withdrawLend, it will only remove the amount returned by the hard/soft vault from pos.underlying amount. If there is a withdraw fee, underlying amount will not be decrease properly and the user will be left with phantom collateral that they can still use.

Vulnerability Detail

```
// Cut withdraw fee if it is in withdrawVaultFee Window (2 months)
if (
    block.timestamp <
    config.withdrawVaultFeeWindowStartTime() +
        config.withdrawVaultFeeWindow()
) {
    uint256 fee = (withdrawAmount * config.withdrawVaultFee()) /
        DENOMINATOR;
    uToken.safeTransfer(config.treasury(), fee);
    withdrawAmount -= fee;
}
```

Both SoftVault and HardVault implement a withdraw fee. Here we see that withdrawAmount (the return value) is decreased by the fee amount.

```
uint256 wAmount;
if (address(ISoftVault(bank.softVault).uToken()) == token) {
    ISoftVault(bank.softVault).approve(
        bank.softVault,
        type(uint256).max
    );
    wAmount = ISoftVault(bank.softVault).withdraw(shareAmount);
} else {
```

```
    wAmount = IHardVault(bank.hardVault).withdraw(token, shareAmount);
}

wAmount = wAmount > pos.underlyingAmount
    ? pos.underlyingAmount
    : wAmount;

pos.underlyingVaultShare -= shareAmount;
pos.underlyingAmount -= wAmount;
bank.totalLend -= wAmount;
```

The return value is stored as `wAmount` which is then subtracted from `pos.underlyingAmount` the issue is that the withdraw fee has now caused a token accounting error for `pos`. We see that the fee paid to the hard/soft vault is NOT properly removed from `pos.underlyingAmount`. This leaves the user with phantom underlying which doesn't actually exist but that the user can use to take out loans.

Exmaple: For simplicity let's say that 1 share = 1 underlying and the soft/hard vault has a fee of 5%. Imagine a user deposits 100 underlying to receive 100 shares. Now the user withdraws their 100 shares while the hard/soft vault has a withdraw. This burns 100 shares and softVault/hardVault.withdraw returns 95 (100 - 5). During the token accounting pos.underlyingVaultShares are decreased to 0 but pos.underlyingAmount is still equal to 5 (100 - 95).

```
uint256 cv = oracle.getUnderlyingValue(
    pos.underlyingToken,
    pos.underlyingAmount
);
```

This accounting error is highly problematic because collateralValue uses pos.underlyingAmount to determine the value of collateral for liquidation purposes. This allows the user to take on more debt than they should.

Impact

User is left with collateral that isn't real but that can be used to take out a loan

Code Snippet

https://github.com/sherlock-audit/2023-02-blueberry/blob/main/contracts/BlueBerryBank.sol#L669-L704

Tool used

Manual Review

Recommendation

`HardVault/SoftVault#withdraw` should also return the fee paid to the vault, so that it can be accounted for.

Issue H-10: IchiLpOracle is extemely easy to manipulate due to how IchiVault calculates underlying token balances

Source: https://github.com/sherlock-audit/2023-02-blueberry-judging/issues/20

Found by

carrot, obront, ctf_sec, cergyk, banditx0x, psy4n0n, 0x52

Summary

`IchiVault#getTotalAmounts` uses the `UniV3Pool.slot0` to determine the number of tokens it has in it's position. `slot0` is the most recent data point and is therefore extremely easy to manipulate. Given that the protocol specializes in leverage, the effects of this manipulation would compound to make malicious uses even easier.

Vulnerability Detail

ICHIVault.sol

```
function _amountsForLiquidity(
    int24 tickLower,
    int24 tickUpper,
    uint128 liquidity
) internal view returns (uint256, uint256) {
    (uint160 sqrtRatioX96, , , , , , ) = IUniswapV3Pool(pool).slot0();
    return
        UV3Math.getAmountsForLiquidity(
            sqrtRatioX96,
            UV3Math.getSqrtRatioAtTick(tickLower),
            UV3Math.getSqrtRatioAtTick(tickUpper),
            liquidity
        );
}
```

`IchiVault#getTotalAmounts` uses the `UniV3Pool.slot0` to determine the number of tokens it has in it's position. slot0 is the most recent data point and can easily be manipulated.

https://github.com/sherlock-audit/2023-02-blueberry/blob/main/contracts/oracle/IchiLpOracle.sol#L27-L36

`IchiLPOracle` directly uses the token values returned by `vault#getTotalAmounts`. This allows a malicious user to manipulate the valuation of the LP. An example of this kind of manipulation would be to use large buys/sells to alter the composition of the LP to make it worth less or more.

Impact

Ichi LP value can be manipulated to cause loss of funds for the protocol and other users

Code Snippet

Tool used

Manual Review

Recommendation

Token balances should be calculated inside the oracle instead of getting them from the `IchiVault`. To determine the liquidity, use a TWAP instead of `slot0`.

Issue M-1: The maximum size of an ICHI vault spell position can be arbitrarily surpassed

Source: https://github.com/sherlock-audit/2023-02-blueberry-judging/issues/327

Found by

berndartmueller, koxuan, rvierdiiev, rbserver

Summary

The maximum size of an ICHI vault spell position can be arbitrarily surpassed by subsequent deposits to a position due to a flaw in the curPosSize calculation.

Vulnerability Detail

Ichi vault spell positions are subject to a maximum size limit to prevent large positions, ensuring a wide margin for liquidators and bad debt prevention for the protocol.

The maximum position size is enforced in the IchiVaultSpell.depositInternal function and compared to the current position size curPosSize.

However, the curPosSize does not reflect the actual position size, but the amount of Ichi vault LP tokens that are currently held in the IchiVaultSpell contract (see L153).

Assets can be repeatedly deposited into an Ichi vault spell position using the IchiVaultSpell.openPosition function (via the BlueBerryBank.execute function).

On the very first deposit, the curPosSize correctly reflects the position size. However, on subsequent deposits, the previously received Ichi vault LP tokens are kept in the BlueBerryBank contract. Thus, checking the balance of vault tokens in the IchiVaultSpell contract only accounts for the current deposit.

Test case

To demonstrate this issue, please use the following test case:

```
diff --git a/test/spell/ichivault.spell.test.ts
↪  b/test/spell/ichivault.spell.test.ts
index 258d653..551a6eb 100644
--- a/test/spell/ichivault.spell.test.ts
+++ b/test/spell/ichivault.spell.test.ts
@@ -163,6 +163,26 @@ describe('ICHI Angel Vaults Spell', () => {
                                afterTreasuryBalance.sub(beforeTreasuryBalance)
                        ).to.be.equal(depositAmount.mul(50).div(10000))
```

```
                })
+               it("should revert when exceeds max pos size due to increasing
↪  position", async () => {
+                       await ichi.approve(bank.address,
↪  ethers.constants.MaxUint256);
+                       await bank.execute(
+                               0,
+                               spell.address,
+                               iface.encodeFunctionData("openPosition", [
+                                       0, ICHI, USDC, depositAmount.mul(4),
↪  borrowAmount.mul(6) // Borrow 1.800e6 USDC
+                               ])
+                       );
+
+                       await expect(
+                               bank.execute(
+                                       0,
+                                       spell.address,
+                                       iface.encodeFunctionData("openPosition",
↪  [
+                                               0, ICHI, USDC,
↪  depositAmount.mul(1), borrowAmount.mul(2) // Borrow 300e6 USDC
+                                       ])
+                               )
+                       ).to.be.revertedWith("EXCEED_MAX_POS_SIZE"); // 1_800e6
↪  + 300e6 = 2_100e6 > 2_000e6 strategy max position size limit
+               })
                it("should be able to return position risk ratio", async () => {
                        let risk = await bank.getPositionRisk(1);
                        console.log('Prev Position Risk',
↪  utils.formatUnits(risk, 2), '%');
```

Run the test with the following command:

```
yarn hardhat test --grep "should revert when exceeds max pos size due to
↪  increasing position"
```

The test case fails and therefore shows that the maximum position size can be exceeded **without reverting**.

Impact

The maximum position size limit can be exceeded, leading to potential issues with liquidations and bad debt accumulation.

Code Snippet

spell/IchiVaultSpell.sol#L152-L156

```
122: function depositInternal(
123:     uint256 strategyId,
124:     address collToken,
125:     address borrowToken,
126:     uint256 collAmount,
127:     uint256 borrowAmount
128: ) internal {
...      // [...]
147:
148:     // 4. Validate MAX LTV
149:     _validateMaxLTV(strategyId);
150:
151:     // 5. Validate Max Pos Size
152:     uint256 lpPrice = bank.oracle().getPrice(strategy.vault);
153:     uint256 curPosSize = (lpPrice * vault.balanceOf(address(this))) /
154:         10**IICHIVault(strategy.vault).decimals();
155:     if (curPosSize > strategy.maxPositionSize)
156:         revert EXCEED_MAX_POS_SIZE(strategyId);
157: }
```

Tool used

Manual Review

Recommendation

Consider determining the current position size using the `bank.getPositionValue()` function instead of using the current Ichi vault LP token balance.

Issue M-2: Liquidations are enabled when repayments are disabled, causing borrowers to lose funds without a chance to repay

Source: https://github.com/sherlock-audit/2023-02-blueberry-judging/issues/290

Found by

Jeiwan, Nyx

Summary

Debt repaying can be temporary disabled by the admin of `BlueBerryBank`, however liquidations are not disabled during this period. As a result, users' positions can accumulate more borrow interest, go above the liquidation threshold, and be liquidated, while users aren't able to repay the debts.

Vulnerability Detail

The owner of BlueBerryBank can disable different functions of the contract, including repayments. However, while repayments are disabled liquidations are still allowed. As a result, when repayments are disabled, liquidator can liquidate any position, and borrowers won't be able to protect against that by repaying their debts. Thus, borrowers will be forced to lose their collateral.

Impact

Positions will be forced to liquidations while their owners won't be able to repay debts to avoid liquidations.

Code Snippet

BlueBerryBank.sol#L740

Tool used

Manual Review

Recommendation

Consider disallowing liquidations when repayments are disabled. Alternatively, consider never disallowing repayments so that users could maintain their positions in a healthy risk range anytime.

Issue M-3: IchiLpOracle returns inflated price due to invalid calculation

Source: https://github.com/sherlock-audit/2023-02-blueberry-judging/issues/254

Found by

sakshamguruji, tives, peanuts

Summary

`IchiLpOracle` returns inflated price due to invalid calculation

Vulnerability Detail

If you run the tests, then you can see that IchiLpOracle returns inflated price for the ICHI_USDC vault

```
STATICCALL
↪  IchiLpOracle.getPrice(token=0xFCFE742e19790Dd67a627875ef8b45F17DB1DaC6) =>
↪  (1101189125194558706411110851447)
```

As the documentation says, the token price should be in USD with 18 decimals of precision. The price returned here is `1101189125194_558706411110851447` This is 1.1 trillion USD when considering the 18 decimals.

The test uses real values except for mocking ichi and usdc price, which are returned by the mock with correct decimals (1e18 and 1e6)

Impact

`IchiLpOracle` price is used in `_validateMaxLTV` (collToken is the vault). Therefore the collateral value is inflated and users can open bigger positions than their collateral would normally allow.

Code Snippet

```
/**
 * @notice Return lp token price in USD, with 18 decimals of precision.
 * @param token The underlying token address for which to get the price.
 * @return Price in USD
 */
function getPrice(address token) external view override returns (uint256) {
    IICHIVault vault = IICHIVault(token);
    uint256 totalSupply = vault.totalSupply();
```

```
    if (totalSupply == 0) return 0;

    address token0 = vault.token0();
    address token1 = vault.token1();

    (uint256 r0, uint256 r1) = vault.getTotalAmounts();
    uint256 px0 = base.getPrice(address(token0));
    uint256 px1 = base.getPrice(address(token1));
    uint256 t0Decimal = IERC20Metadata(token0).decimals();
    uint256 t1Decimal = IERC20Metadata(token1).decimals();

    uint256 totalReserve = (r0 * px0) /
        10**t0Decimal +
        (r1 * px1) /
        10**t1Decimal;

    return (totalReserve * 1e18) / totalSupply;
}
```

link

Tool used

Manual Review

Recommendation

Fix the LP token price calculation. The problem is that you multiply totalReserve with extra 1e18 (`return (totalReserve * 1e18) / totalSupply;`).

Discussion

Gornutz

duplicate of 15

Issue M-4: Deposit Theft by Crashing LP Spot Prices Through MEV

Source: https://github.com/sherlock-audit/2023-02-blueberry-judging/issues/220

Found by

Robert

Summary

When depositing into an Ichi vault it allows a user to deposit all in a single token and determines the amount of vault shares they receive based off the price of that token in the second. This does not use twap but rather a combination of spot and twap in which it chooses the lesser of the two. There's protection against heavy manipulation occurring all on one block by checking if the difference between the two is greater than 5%, and failing if it is and if the last price change happened on the current block, but if the last price change was on a previous block it does not revert.

Multi-block MEV allows malicious actors to manipulate price over multiple blocks with no risk at all. They can easily manipulate token price down to near 0 on one block, a user tries to deposit on the next and gets almost $0 worth of vault shares for their tokens, vault shareholders pocket the extra tokens from the user's deposit, and token price is returned. With this, a user depositing into Blueberry could have their entire deposit stolen by a malicious actor.

This is fairly easy to do now if you see your own block coming up, manipulate price through MEV on the block before that, then include victim transaction and repayment on your own block right after that (not technically needing MMEV). It will be even easier in the future when MMEV is included in Flashbots.

Vulnerability Detail

0. Malicious attacker has validator or uses MMEV through flashbots.
1. Directly before a block they fully control, the validator manipulates token0 price in the LP pool to next to nothing.
2. On the next block, attacker flash loans a large amount of tokens to purchase Ichi Vault shares.
3. Attacker includes all pending user deposits into the pool that use that token. Each of these returns to the user almost nothing.
4. Attacker withdraws shares and included are the tokens that were stolen from users.

Impact

User deposits will be stolen.

Code Snippet

Price check only reverting on a large change if the block is the same as now: https://etherscan.io/token/0x2a8E09552782563f7A076ccec0Ff39473B91Cd8F#code#L2807

Amount of shares relying on price: https://etherscan.io/token/0x2a8E09552782563f7A076ccec0Ff39473B91Cd8F#code#L2829

Tool used

Manual Review

Recommendation

Check spot and twap price the same way IchiVault does but ensure they are within an allowed delta regardless of when price was last updated.

Discussion

SergeKireev

Escalate for 31 USDC

This strategy is invalid since the validator would expose a big amount of their own funds(*) to being arbitraged away during the block before the one they control (they imbalance the pool during a block which they do not control according to the report). Since generalized MEV searchers are highly efficient the probability of the validator losing their funds in that exact block is higher than not.

(*) They have to use their own funds in the first block because flash loan cannot be used accross blocks obviously

For this attack to work the validator would need to control fully two consecutive blocks, which makes it highely unlikely and thus the risk should be considered very low (comparable to for example continued price manipulation of uniswap pools).

sherlock-admin

> Escalate for 31 USDC
>
> This strategy is invalid since the validator would expose a big amount of their own funds(*) to being arbitraged away during the block before the one they control (they imbalance the pool during a block which they do not control according to the report). Since generalized MEV searchers

> are highly efficient the probability of the validator losing their funds in that exact block is higher than not.
>
> (*) They have to use their own funds in the first block because flash loan cannot be used accross blocks obviously
>
> For this attack to work the validator would need to control fully two consecutive blocks, which makes it highely unlikely and thus the risk should be considered very low (comparable to for example continued price manipulation of uniswap pools).

You've created a valid escalation for 31 USDC!

To remove the escalation from consideration: Delete your comment. To change the amount you've staked on this escalation: Edit your comment **(do not create a new comment)**.

You may delete or edit your escalation comment anytime before the 48-hour escalation window closes. After that, the escalation becomes final.

hrishibhat

Escalation accepted

While this issue is not invalid, accepting this escalation on the basis of lowering the impact of this issue. After discussing internally, given the complex nature of the attack as well precondition of a controlling multi-block MEV & the requirement that attacker would have to use large amounts of their own funds to be able to execute this, considering this issue as a Valid Medium

sherlock-admin

> Escalation accepted
>
> While this issue is not invalid, accepting this escalation on the basis of lowering the impact of this issue. After discussing internally, given the complex nature of the attack as well precondition of a controlling multi-block MEV & the requirement that attacker would have to use large amounts of their own funds to be able to execute this, considering this issue as a Valid Medium

This issue's escalations have been accepted!

Contestants' payouts and scores will be updated according to the changes made on this issue.

Issue M-5: `BlueBerryBank.withdrawLend` function cannot be paused

Source: https://github.com/sherlock-audit/2023-02-blueberry-judging/issues/204

Found by

rbserver

Summary

When an extreme market condition occurs, the protocol faces an exploit, or the authority issues a legal requirement, the protocol is able to pause the lending, borrowing, and repaying functionalities. However, the protocol is unable to pause the functionality for reducing a position.

Vulnerability Detail

Because the `BlueBerryBank` contract does not have a function, which is like `BlueBerryBank.isBorrowAllowed`, `BlueBerryBank.isRepayAllowed`, and `BlueBerryBank.isLendAllowed`, for pausing the functionality for reducing a position, the `BlueBerryBank.withdrawLend` function, which is shown in the Code Snippet section, cannot be paused. Users can still call the `IchiVaultSpell.reducePosition` function that further calls the `BlueBerryBank.withdrawLend` function to reduce a position when there is a need for pausing this functionality.

Impact

Just like pausing the lending, borrowing, and repaying functionalities, it is possible that the protocol needs to pause the functionality for reducing a position. However, when this need occurs, users can still reduce their positions through calling the `IchiVaultSpell.reducePosition` and `BlueBerryBank.withdrawLend` functions. The protocol cannot stop the outflow of the funds due to these position reductions even it is required to do so in this situation.

Code Snippet

https://github.com/sherlock-audit/2023-02-blueberry/blob/main/contracts/spell/IchiVaultSpell.sol#L266-L274

```
function reducePosition(
    uint256 strategyId,
    address collToken,
    uint256 collAmount
) external {
```

```
    doWithdraw(collToken, collAmount);
    doRefund(collToken);
    _validateMaxLTV(strategyId);
}
```

https://github.com/sherlock-audit/2023-02-blueberry/blob/main/contracts/BlueBerryBank.sol#L669-L704

```
function withdrawLend(address token, uint256 shareAmount)
    external
    override
    inExec
    poke(token)
{
    Position storage pos = positions[POSITION_ID];
    Bank storage bank = banks[token];
    if (token != pos.underlyingToken) revert INVALID_UTOKEN(token);
    if (shareAmount == type(uint256).max) {
        shareAmount = pos.underlyingVaultShare;
    }

    uint256 wAmount;
    if (address(ISoftVault(bank.softVault).uToken()) == token) {
        ISoftVault(bank.softVault).approve(
            bank.softVault,
            type(uint256).max
        );
        wAmount = ISoftVault(bank.softVault).withdraw(shareAmount);
    } else {
        wAmount = IHardVault(bank.hardVault).withdraw(token, shareAmount);
    }

    wAmount = wAmount > pos.underlyingAmount
        ? pos.underlyingAmount
        : wAmount;

    pos.underlyingVaultShare -= shareAmount;
    pos.underlyingAmount -= wAmount;
    bank.totalLend -= wAmount;

    wAmount = doCutWithdrawFee(token, wAmount);

    IERC20Upgradeable(token).safeTransfer(msg.sender, wAmount);
}
```

Tool used

Manual Review

Recommendation

A function, which is similar to the `BlueBerryBank.isBorrowAllowed`, `BlueBerryBank.isRepayAllowed`, and `BlueBerryBank.isLendAllowed` functions, can be added in the `BlueBerryBank` contract for pausing the `BlueBerryBank.withdrawLend` function. This function can then be used in the `BlueBerryBank.withdrawLend` function so the `BlueBerryBank.withdrawLend` function can be paused when needed.

Issue M-6: If a token's oracle goes down or price falls to zero, liquidations will be frozen

Source: https://github.com/sherlock-audit/2023-02-blueberry-judging/issues/161

Found by

8olidity, 0xChinedu, rvierdiiev, obront, sakshamguruji, Saeedalipoor01988

Summary

In some extreme cases, oracles can be taken offline or token prices can fall to zero. In these cases, liquidations will be frozen (all calls will revert) for any debt holders holding this token, even though they may be some of the most important times to allow liquidations to retain the solvency of the protocol.

Vulnerability Detail

Chainlink has taken oracles offline in extreme cases. For example, during the UST collapse, Chainlink paused the UST/ETH price oracle, to ensure that it wasn't providing inaccurate data to protocols.

In such a situation (or one in which the token's value falls to zero), all liquidations for users holding the frozen asset would revert. This is because any call to `liquidate()` calls `isLiquidatable()`, which calls `getPositionRisk()`, which calls the oracle to get the values of all the position's tokens (underlying, debt, and collateral).

Depending on the specifics, one of the following checks would cause the revert:

- the call to Chainlink's `registry.latestRoundData` would fail
- `if (updatedAt < block.timestamp - maxDelayTime) revert PRICE_OUTDATED(_token);`
- `if (px == 0) revert PRICE_FAILED(token);`

If the oracle price lookup reverts, liquidations will be frozen, and the user will be immune to liquidations. Although there are ways this could be manually fixed with fake oracles, by definition this happening would represent a cataclysmic time where liquidations need to be happening promptly to avoid the protocol falling into insolvency.

Impact

Liquidations may not be possible at a time when the protocol needs them most. As a result, the value of user's asset may fall below their debts, turning off any liquidation incentive and pushing the protocol into insolvency.

Code Snippet

https://github.com/sherlock-audit/2023-02-blueberry/blob/main/contracts/BlueBerryBank.sol#L511-L517

https://github.com/sherlock-audit/2023-02-blueberry/blob/main/contracts/BlueBerryBank.sol#L497-L505

https://github.com/sherlock-audit/2023-02-blueberry/blob/main/contracts/BlueBerryBank.sol#L477-L488

https://github.com/sherlock-audit/2023-02-blueberry/blob/main/contracts/oracle/CoreOracle.sol#L182-L189

https://github.com/sherlock-audit/2023-02-blueberry/blob/main/contracts/oracle/CoreOracle.sol#L95-L99

https://github.com/sherlock-audit/2023-02-blueberry/blob/main/contracts/oracle/ChainlinkAdapterOracle.sol#L66-L84

Tool used

Manual Review

Recommendation

Ensure there is a safeguard in place to protect against this possibility.

Issue M-7: totalLend isn't updated on liquidation, leading to permanently inflated value

Source: https://github.com/sherlock-audit/2023-02-blueberry-judging/issues/155

Found by

berndartmueller, obront, SPYBOY, cducrest-brainbot

Summary

`bank.totalLend` tracks the total amount that has been lent of a given token, but it does not account for tokens that are withdrawn when a position is liquidated. As a result, the value will become overstated, leading to inaccurate data on the pool.

Vulnerability Detail

When a user lends a token to the Compound fork, the bank for that token increases its `totalLend` parameter:

```
bank.totalLend += amount;
```

Similarly, this value is decreased when the amount is withdrawn.

In the event that a position is liquidated, the `underlyingAmount` and `underlyingVaultShare` for the user are decreased based on the amount that will be transferred to the liquidator.

```
uint256 liqSize = (pos.collateralSize * share) / oldShare;
uint256 uTokenSize = (pos.underlyingAmount * share) / oldShare;
uint256 uVaultShare = (pos.underlyingVaultShare * share) / oldShare;

pos.collateralSize -= liqSize;
pos.underlyingAmount -= uTokenSize;
pos.underlyingVaultShare -= uVaultShare;
```

However, the liquidator doesn't receive those shares "inside the system". Instead, they receive the softVault tokens that can be claimed directly for the underlying asset by calling `withdraw()`, which simply redeems the underlying tokens from the Compound fork and sends them to the user.

```
function withdraw(uint256 shareAmount)
    external
    override
    nonReentrant
    returns (uint256 withdrawAmount)
```

```
{
    if (shareAmount == 0) revert ZERO_AMOUNT();

    _burn(msg.sender, shareAmount);

    uint256 uBalanceBefore = uToken.balanceOf(address(this));
    if (cToken.redeem(shareAmount) != 0) revert REDEEM_FAILED(shareAmount);
    uint256 uBalanceAfter = uToken.balanceOf(address(this));

    withdrawAmount = uBalanceAfter - uBalanceBefore;
    // Cut withdraw fee if it is in withdrawVaultFee Window (2 months)
    if (
        block.timestamp <
        config.withdrawVaultFeeWindowStartTime() +
            config.withdrawVaultFeeWindow()
    ) {
        uint256 fee = (withdrawAmount * config.withdrawVaultFee()) /
            DENOMINATOR;
        uToken.safeTransfer(config.treasury(), fee);
        withdrawAmount -= fee;
    }
    uToken.safeTransfer(msg.sender, withdrawAmount);

    emit Withdrawn(msg.sender, withdrawAmount, shareAmount);
}
```

Nowhere in this process is `bank.totalLend` updated. As a result, each time there is a liquidation of size X, `bank.totalLend` will move X higher relative to the correct value. Slowly, over time, this value will begin to dramatically misrepresent the accurate amount that has been lent.

While there is no material exploit based on this inaccuracy at the moment, this is a core piece of data in the protocol, and it's inaccuracy could lead to major issues down the road.

Furthermore, it will impact immediate user behavior, as the Blueberry devs have explained "we use that [value] to help us display TVL with subgraph", which will deceive and confuse users.

Impact

A core metric of the protocol will be permanently inaccurate, giving users incorrect data to make their assessments on and potentially causing more severe issues down the road.

Code Snippet

https://github.com/sherlock-audit/2023-02-blueberry/blob/main/contracts/BlueBerryBank.sol#L511-L572

https://github.com/sherlock-audit/2023-02-blueberry/blob/main/contracts/vault/SoftVault.sol#L94-L123

Tool used

Manual Review

Recommendation

For the best accuracy, updating `bank.totalLend` should happen from the `withdraw()` function in `SoftVault.sol` instead of from the core `BlueberryBank.sol` contract.

Alternatively, you could add an update to `bank.totalLend` in the `liquidate()` function, which might temporarily underrepresent the total lent before the liquidator withdrew the funds, but would end up being accurate over the long run.

Issue M-8: Complete debt size is not paid off for fee on transfer tokens, but users aren't warned

Source: https://github.com/sherlock-audit/2023-02-blueberry-judging/issues/153

Found by

tsvetanovv, rvierdiiev, Avci, obront, chaduke, berndartmueller, Breeje

Summary

The protocol seems to be intentionally catering to fee on transfer tokens by measuring token balances before and after transfers to determine the value received. However, the mechanism to pay the full debt will not succeed in paying off the debt if it is used with a fee on transfer token.

Vulnerability Detail

The protocol is clearly designed to ensure it is compatible with fee on transfer tokens. For example, all functions that receive tokens check the balance before and after, and calculate the difference between these values to measure tokens received:

```
function doERC20TransferIn(address token, uint256 amountCall)
    internal
    returns (uint256)
{
    uint256 balanceBefore = IERC20Upgradeable(token).balanceOf(
        address(this)
    );
    IERC20Upgradeable(token).safeTransferFrom(
        msg.sender,
        address(this),
        amountCall
    );
    uint256 balanceAfter = IERC20Upgradeable(token).balanceOf(
        address(this)
    );
    return balanceAfter - balanceBefore;
}
```

There is another feature of the protocol, which is that when loans are being repaid, the protocol gives the option of passing `type(uint256).max` to pay your debt in full:

```
if (amountCall == type(uint256).max) {
    amountCall = oldDebt;
```

```
}
```

However, these two features are not compatible. If a user paying off fee on transfer tokens passes in `type(uint256).max` to pay their debt in full, the full amount of their debt will be calculated. But when that amount is transferred to the contract, the amount that the result increases will be slightly less. As a result, the user will retain some balance that is not paid off.

Impact

The feature to allow loans to be paid in full will silently fail when used with fee on transfer tokens, which may trick users into thinking they have completely paid off their loans, and accidentally maintaining a balance.

Code Snippet

https://github.com/sherlock-audit/2023-02-blueberry/blob/main/contracts/BlueBerryBank.sol#L760-L775

Tool used

Manual Review

Recommendation

I understand that it would be difficult to implement a mechanism to pay fee on transfer tokens off in full. That adds a lot of complexity that is somewhat fragile.

The issue here is that the failure is silent, so that users request to pay off their loan in full, get confirmation, and may not realize that the loan still has an outstanding balance with interest accruing.

To solve this, there should be a confirmation that any user who passes `type(uint256).max` has paid off their debt in full. Otherwise, the function should revert, so that users paying fee on transfer tokens know that they cannot use the "pay in full" feature and must specify the correct amount to get their outstanding balance down to zero.

Issue M-9: LP tokens cannot be valued because ICHI cannot be priced by oracle, causing all new open positions to revert

Source: https://github.com/sherlock-audit/2023-02-blueberry-judging/issues/152

Found by

obront

Summary

In order to value ICHI LP tokens, the oracle uses the Fair LP Pricing technique, which uses the prices of both individual tokens, along with the quantities, to calculate the LP token value. However, this process requires the underlying token prices to be accessible by the oracle. Both Chainlink and Band do not support the ICHI token, so the function will fail, causing all new positions using the IchiVaultSpell to revert.

Vulnerability Detail

When a new Ichi position is opened, the ICHI LP tokens are posted as collateral. Their value is assessed using the `IchiLpOracle#getPrice()` function:

```
function getPrice(address token) external view override returns (uint256) {
    IICHIVault vault = IICHIVault(token);
    uint256 totalSupply = vault.totalSupply();
    if (totalSupply == 0) return 0;

    address token0 = vault.token0();
    address token1 = vault.token1();

    (uint256 r0, uint256 r1) = vault.getTotalAmounts();
    uint256 px0 = base.getPrice(address(token0));
    uint256 px1 = base.getPrice(address(token1));
    uint256 t0Decimal = IERC20Metadata(token0).decimals();
    uint256 t1Decimal = IERC20Metadata(token1).decimals();

    uint256 totalReserve = (r0 * px0) /
        10**t0Decimal +
        (r1 * px1) /
        10**t1Decimal;

    return (totalReserve * 1e18) / totalSupply;
}
```

This function uses the "Fair LP Pricing" formula, made famous by Alpha Homora. To simplify, this uses an oracle to get the prices of both underlying tokens, and then calculates the LP price based on these values and the reserves.

However, this process requires that we have a functioning oracle for the underlying tokens. However, Chainlink and Band both do not support the ICHI token (see the links for their comprehensive lists of data feeds). As a result, the call to `base.getPrice(token0)` will fail.

All prices are calculated in the `isLiquidatable()` check at the end of the `execute()` function. As a result, any attempt to open a new ICHI position and post the LP tokens as collateral (which happens in both `openPosition()` and `openPositionFarm()`) will revert.

Impact

All new positions opened using the `IchiVaultSpell` will revert when they attempt to look up the LP token price, rendering the protocol useless.

Code Snippet

https://github.com/sherlock-audit/2023-02-blueberry/blob/main/contracts/oracle/IchiLpOracle.sol#L19-L39

Tool used

Manual Review

Recommendation

There will need to be an alternate form of oracle that can price the ICHI token. The best way to accomplish this is likely to use a TWAP of the price on an AMM.

Discussion

Gornutz

There is additional oracles for assets not supported by chainlink or band but just not in scope of this specific audit.

hrishibhat

Based on the context there are no implementations for getting the price of the ICHI token. Considering this a valid issue.

SergeKireev

Escalate for 31 USDC

Impact stated is medium, since positions cannot be opened and no funds are at risk. The high severity definition as stated per Sherlock docs:

> This vulnerability would result in a material loss of funds and the cost of the attack is low (relative to the amount of funds lost). The attack path is possible with reasonable assumptions that mimic on-chain conditions. The vulnerability must be something that is not considered an acceptable risk by a reasonable protocol team.

sherlock-admin

> Escalate for 31 USDC
>
> Impact stated is medium, since positions cannot be opened and no funds are at risk. The high severity definition as stated per Sherlock docs:
>
> > This vulnerability would result in a material loss of funds and the cost of the attack is low (relative to the amount of funds lost). The attack path is possible with reasonable assumptions that mimic on-chain conditions. The vulnerability must be something that is not considered an acceptable risk by a reasonable protocol team.

You've created a valid escalation for 31 USDC!

To remove the escalation from consideration: Delete your comment. To change the amount you've staked on this escalation: Edit your comment **(do not create a new comment)**.

You may delete or edit your escalation comment anytime before the 48-hour escalation window closes. After that, the escalation becomes final.

hrishibhat

Escalation accepted

This is a valid medium Also Given that this is an issue only for the Ichi tokens and impact is only unable to open positions.

sherlock-admin

> Escalation accepted
>
> This is a valid medium Also Given that this is an issue only for the Ichi tokens and impact is only unable to open positions.

This issue's escalations have been accepted!

Contestants' payouts and scores will be updated according to the changes made on this issue.

Issue M-10: HardVault never deposits assets to Compound

Source: https://github.com/sherlock-audit/2023-02-blueberry-judging/issues/147

Found by

obront, koxuan

Summary

While the protocol states that all underlying assets are deposited to their Compound fork to earn interest, it appears this action never happens in `HardVault.sol`.

Vulnerability Detail

The documentation and comments seem to make clear that all assets deposited to `HardVault.sol` should be deposited to Compound to earn yield:

```
/**
    * @notice Deposit underlying assets on Compound and issue share token
    * @param amount Underlying token amount to deposit
    * @return shareAmount cToken amount
    */
function deposit(address token, uint256 amount) { ... }

/**
    * @notice Withdraw underlying assets from Compound
    * @param shareAmount Amount of cTokens to redeem
    * @return withdrawAmount Amount of underlying assets withdrawn
    */
function withdraw(address token, uint256 shareAmount) { ... }
```

However, if we examine the code in these functions, there is no movement of the assets to Compound. Instead, they sit in the Hard Vault and doesn't earn any yield.

Impact

Users who may expect to be earning yield on their underlying tokens will not be.

Code Snippet

https://github.com/sherlock-audit/2023-02-blueberry/blob/main/contracts/vault/HardVault.sol#L68-L116

Tool used

Manual Review

Recommendation

Either add the functionality to the Hard Vault to have the assets pulled from the ERC1155 and deposited to the Compound fork, or change the comments and docs to be clear that such underlying assets will not be receiving any yield.

Issue M-11: Withdrawals from IchiVaultSpell have no slippage protection so can be frontrun, stealing all user funds

Source: https://github.com/sherlock-audit/2023-02-blueberry-judging/issues/130

Found by

rvierdiiev, obront, koxuan, ctf_sec, tives, cergyk, berndartmueller, 0x52

Summary

When a user withdraws their position through the `IchiVaultSpell`, part of the unwinding process is to trade one of the released tokens for the other, so the borrow can be returned. This trade is done on Uniswap V3. The parameters are set in such a way that there is no slippage protection, so any MEV bot could see this transaction, aggressively sandwich attack it, and steal the majority of the user's funds.

Vulnerability Detail

Users who have used the `IchiVaultSpell` to take positions in Ichi will eventually choose to withdraw their funds. They can do this by calling `closePosition()` or `closePositionFarm()`, both of which call to `withdrawInternal()`, which follows loosely the following logic:

- sends the LP tokens back to the Ichi vault for the two underlying tokens (one of which was what was borrowed)
- swaps the non-borrowed token for the borrowed token on UniV3, to ensure we will be able to pay the loan back
- withdraw our underlying token from the Compound fork
- repay the borrow token loan to the Compound fork
- validate that we are still under the maxLTV for our strategy
- send the funds (borrow token and underlying token) back to the user

The issue exists in the swap, where Uniswap is called with the following function:

```
if (amountToSwap > 0) {
    swapPool = IUniswapV3Pool(vault.pool());
    swapPool.swap(
        address(this),
        !isTokenA,
        int256(amountToSwap),
        isTokenA
```

```
            ? UniV3WrappedLibMockup.MAX_SQRT_RATIO - 1
            : UniV3WrappedLibMockup.MIN_SQRT_RATIO + 1,
        abi.encode(address(this))
    );
}
```

The 4th variable is called `sqrtPriceLimitX96` and it represents the square root of the lowest or highest price that you are willing to perform the trade at. In this case, we've hardcoded in that we are willing to take the worst possible rate (highest price in the event we are trading 1 => 0; lowest price in the event we are trading 0 => 1).

The `IchiVaultSpell.sol#uniswapV3SwapCallback()` function doesn't enforce any additional checks. It simply sends whatever delta is requested directly to Uniswap.

```
function uniswapV3SwapCallback(
    int256 amount0Delta,
    int256 amount1Delta,
    bytes calldata data
) external override {
    if (msg.sender != address(swapPool)) revert NOT_FROM_UNIV3(msg.sender);
    address payer = abi.decode(data, (address));

    if (amount0Delta > 0) {
        if (payer == address(this)) {
            IERC20Upgradeable(swapPool.token0()).safeTransfer(
                msg.sender,
                uint256(amount0Delta)
            );
        } else {
            IERC20Upgradeable(swapPool.token0()).safeTransferFrom(
                payer,
                msg.sender,
                uint256(amount0Delta)
            );
        }
    } else if (amount1Delta > 0) {
        if (payer == address(this)) {
            IERC20Upgradeable(swapPool.token1()).safeTransfer(
                msg.sender,
                uint256(amount1Delta)
            );
        } else {
            IERC20Upgradeable(swapPool.token1()).safeTransferFrom(
                payer,
                msg.sender,
                uint256(amount1Delta)
            );
        }
```

```
    }
}
```

While it is true that there is an `amountRepay` parameter that is inputted by the user, it is not sufficient to protect users. Many users will want to make only a small repayment (or no repayment) while unwinding their position, and thus this variable will only act as slippage protection in the cases where users intend to repay all of their returned funds.

With this knowledge, a malicious MEV bot could watch for these transactions in the mempool. When it sees such a transaction, it could perform a "sandwich attack", trading massively in the same direction as the trade in advance of it to push the price out of whack, and then trading back after us, so that they end up pocketing a profit at our expense.

Because many of the ICHI token pairs have small amounts of liquidity (for example, ICHI-WBTC has under $350k), such an attack could feasible take the majority of the funds, leaving the user with close to nothing. See more details on liquidity here: https://info.uniswap.org/#/tokens/0x111111517e4929d3dcbdfa7cce55d30d4b6bc4d6

Impact

Users withdrawing their funds through the `IchiVaultSpell` who do not plan to repay all of the tokens returned from Uniswap could be sandwich attacked, losing their funds by receiving very little of their borrowed token back from the swap.

Code Snippet

https://github.com/sherlock-audit/2023-02-blueberry/blob/main/contracts/spell/IchiVaultSpell.sol#L300-L317

https://github.com/sherlock-audit/2023-02-blueberry/blob/main/contracts/spell/IchiVaultSpell.sol#L407-L442

Tool used

Manual Review

Recommendation

Have the user input a slippage parameter to ensure that the amount of borrowed token they receive back from Uniswap is in line with what they expect.

Alternatively, use the existing oracle system to estimate a fair price and use that value in the `swap()` call.

Issue M-12: Chainlink's latestRoundData return stale or incorrect result

Source: https://github.com/sherlock-audit/2023-02-blueberry-judging/issues/94

Found by

8olidity, tsvetanovv, WatchDogs, Nyx, Avci, obront, Aymen0909, SPYBOY, HonorLt, csanuragjain, koxuan, evan, rbserver, hl_, peanuts, Chinmay

Summary

https://github.com/sherlock-audit/2023-02-blueberry/blob/main/contracts/oracle/ChainlinkAdapterOracle.sol#L76

Vulnerability Detail

Impact

On ChainlinkAdapterOracle.sol, you are using latestRoundData, but there is no check if the return value indicates stale data.

```
function getPrice(address _token) external view override returns (uint256) {
        // remap token if possible
        address token = remappedTokens[_token];
        if (token == address(0)) token = _token;

        uint256 maxDelayTime = maxDelayTimes[token];
        if (maxDelayTime == 0) revert NO_MAX_DELAY(_token);

        // try to get token-USD price
        uint256 decimals = registry.decimals(token, USD);
        (, int256 answer, , uint256 updatedAt, ) = registry.latestRoundData(
            token,
            USD
        );
        if (updatedAt < block.timestamp - maxDelayTime)
            revert PRICE_OUTDATED(_token);

        return (answer.toUint256() * 1e18) / 10**decimals;
    }
```

This could lead to stale prices according to the Chainlink documentation: https://docs.chain.link/data-feeds/price-feeds/historical-data Related report: https://github.com/code-423n4/2021-05-fairside-findings/issues/70

Code Snippet

https://github.com/sherlock-audit/2023-02-blueberry/blob/main/contracts/oracle/ChainlinkAdapterOracle.sol#L76

Tool used

Manual Review

Recommendation

Add the below check for returned data

```
function getPrice(address _token) external view override returns (uint256) {
        // remap token if possible
        address token = remappedTokens[_token];
        if (token == address(0)) token = _token;

        uint256 maxDelayTime = maxDelayTimes[token];
        if (maxDelayTime == 0) revert NO_MAX_DELAY(_token);

        // try to get token-USD price
        uint256 decimals = registry.decimals(token, USD);
        (uint80 roundID, int256 answer, uint256 timestamp, uint256 updatedAt, )
↪   = registry.latestRoundData(
            token,
            USD
        );
        //Solution
        require(updatedAt >= roundID, "Stale price");
        require(timestamp != 0,"Round not complete");
        require(answer > 0,"Chainlink answer reporting 0");

        if (updatedAt < block.timestamp - maxDelayTime)
            revert PRICE_OUTDATED(_token);

        return (answer.toUint256() * 1e18) / 10**decimals;
    }
```

Issue M-13: BasicSpell.doCutRewardsFee uses depositFee instead of withdraw fee

Source: https://github.com/sherlock-audit/2023-02-blueberry-judging/issues/82

Found by

rvierdiiev

Summary

BasicSpell.doCutRewardsFee uses depositFee instead of withdraw fee

Vulnerability Detail

https://github.com/sherlock-audit/2023-02-blueberry/blob/main/contracts/spell/BasicSpell.sol#L65-L79

```
function doCutRewardsFee(address token) internal {
    if (bank.config().treasury() == address(0)) revert NO_TREASURY_SET();


    uint256 balance = IERC20Upgradeable(token).balanceOf(address(this));
    if (balance > 0) {
        uint256 fee = (balance * bank.config().depositFee()) / DENOMINATOR;
        IERC20Upgradeable(token).safeTransfer(
            bank.config().treasury(),
            fee
        );


        balance -= fee;
        IERC20Upgradeable(token).safeTransfer(bank.EXECUTOR(), balance);
    }
}
```

This function is called in order to get fee from ICHI rewards, collected by farming. But currently it takes `bank.config().depositFee()` instead of `bank.config().withdrawFee()`.

Impact

Wrong fee amount is taken.

Code Snippet

https://github.com/sherlock-audit/2023-02-blueberry/blob/main/contracts/spell/BasicSpell.sol#L65-L79

Tool used

Manual Review

Recommendation

Take withdraw fee from rewards.

Issue M-14: A borrower might drain the vault by calling borrow() repeatedly with small borrow amount each time.

Source: https://github.com/sherlock-audit/2023-02-blueberry-judging/issues/45

Found by

chaduke

Summary

A borrower might drain the vault by calling `borrow()` repeatedly with small borrow amount that converts to a zero debt share each time.

Vulnerability Detail

This is possible because `borrow()` does not check whether the number of shares borrowed is equal to zero or not. Therefore, an attacker can take advantage of the rounding error and borrow funds for free. We show how a borrowed can drain the vault by calling borrow() repeatedly:

1) Suppose the for a particular token X, the total bank debt is 1000,000 and the total debt share is 100,000. That is each debt share has a 10 debt.
2) A malicious borrower Bob can call `borrow()` (via SPELL) and borrow 9 each time, which will convert to `9*100,000/1000,000 = 0` debt shares.

https://github.com/sherlock-audit/2023-02-blueberry/blob/main/contracts/BlueBerryBank.sol#L709-L735

3) As a result, the borrower can steal 9 X tokens each time the `borrow()` is called without increasing his debt shares. Bob can call this repeatedly in one transaction `Steal()` (within the gas limit) to borrow many tokens of X without increasing any debt shares.
4) Call `Steal()` many times, Bob will be able to drain the vault.

Impact

A malicious borrower can drain the the vault by calling `borrow()` repeatedly.

Code Snippet

See above

Tool used

VScode Manual Review

Recommendation

Borrow should revert when `newShare == 0`.

```
 function borrow(address token, uint256 amount)
        external
        override
        inExec
        poke(token)
        onlyWhitelistedToken(token)
    {
        if (!isBorrowAllowed()) revert BORROW_NOT_ALLOWED();
        Bank storage bank = banks[token];
        Position storage pos = positions[POSITION_ID];
        uint256 totalShare = bank.totalShare;
        uint256 totalDebt = bank.totalDebt;
        uint256 share = totalShare == 0
            ? amount
            : (amount * totalShare).divCeil(totalDebt);
+       if(share == 0) revert BorrowZeroShare();

        bank.totalShare += share;
        uint256 newShare = pos.debtShareOf[token] + share;
        pos.debtShareOf[token] = newShare;
        if (newShare > 0) {
            pos.debtMap |= (1 << uint256(bank.index));
        }
        IERC20Upgradeable(token).safeTransfer(
            msg.sender,
            doBorrow(token, amount)
        );
        emit Borrow(POSITION_ID, msg.sender, token, amount, share);
    }
```

Issue M-15: onlyEOAEx modifier that ensures call is from EOA might not hold true in the future

Source: https://github.com/sherlock-audit/2023-02-blueberry-judging/issues/21

Found by

koxuan

Summary

modifier `onlyEOAEx` is used to ensure calls are only made from EOA. However, EIP 3074 suggests that using `onlyEOAEx` modifier to ensure calls are only from EOA might not hold true.

Vulnerability Detail

For `onlyEOAEx`, `tx.origin` is used to ensure that the caller is from an EOA and not a smart contract.

```
modifier onlyEOAEx() {
    if (!allowContractCalls && !whitelistedContracts[msg.sender]) {
        if (msg.sender != tx.origin) revert NOT_EOA(msg.sender);
    }
    _;
}
```

However, according to EIP 3074,

This EIP introduces two EVM instructions AUTH and AUTHCALL. The first sets a context variable authorized based on an ECDSA signature. The second sends a call as the authorized account. This essentially delegates control of the externally owned account (EOA) to a smart contract.

Therefore, using tx.origin to ensure msg.sender is an EOA will not hold true in the event EIP 3074 goes through.

Impact

Using modifier `onlyEOAEx` to ensure calls are made only from EOA will not hold true in the event EIP 3074 goes through.

Code Snippet

BlueBerryBank.sol#L54-L59

Tool used

Manual Review

Recommendation

Recommend using OpenZepellin's `isContract` function (https://docs.openzeppelin.com/contracts/2.x/api/utils#Address-isContract-address-). Note that there are edge cases like contract in constructor that can bypass this and hence caution is required when using this.

```
modifier onlyEOAEx() {
    if (!allowContractCalls && !whitelistedContracts[msg.sender]) {
        if (isContract(msg.sender)) revert NOT_EOA(msg.sender);
    }
    _;
}
```

Issue M-16: ChainlinkAdapterOracle will return the wrong price for asset if underlying aggregator hits minAnswer

Source: https://github.com/sherlock-audit/2023-02-blueberry-judging/issues/18

Found by

0x52

Summary

Chainlink aggregators have a built in circuit breaker if the price of an asset goes outside of a predetermined price band. The result is that if an asset experiences a huge drop in value (i.e. LUNA crash) the price of the oracle will continue to return the minPrice instead of the actual price of the asset. This would allow user to continue borrowing with the asset but at the wrong price. This is exactly what happened to Venus on BSC when LUNA imploded.

Vulnerability Detail

ChainlinkAdapterOracle uses the ChainlinkFeedRegistry to obtain the price of the requested tokens.

```
function latestRoundData(
  address base,
  address quote
)
  external
  view
  override
  checkPairAccess()
  returns (
    uint80 roundId,
    int256 answer,
    uint256 startedAt,
    uint256 updatedAt,
    uint80 answeredInRound
  )
{
  uint16 currentPhaseId = s_currentPhaseId[base][quote];
  //@audit this pulls the Aggregator for the requested pair
  AggregatorV2V3Interface aggregator = _getFeed(base, quote);
  require(address(aggregator) != address(0), "Feed not found");
  (
    roundId,
    answer,
```

```
    startedAt,
    updatedAt,
    answeredInRound
  ) = aggregator.latestRoundData();
  return _addPhaseIds(roundId, answer, startedAt, updatedAt, answeredInRound,
  ↪  currentPhaseId);
}
```

ChainlinkFeedRegistry#latestRoundData pulls the associated aggregator and requests round data from it. ChainlinkAggregators have minPrice and maxPrice circuit breakers built into them. This means that if the price of the asset drops below the minPrice, the protocol will continue to value the token at minPrice instead of it's actual value. This will allow users to take out huge amounts of bad debt and bankrupt the protocol.

Example: TokenA has a minPrice of $1. The price of TokenA drops to $0.10. The aggregator still returns $1 allowing the user to borrow against TokenA as if it is $1 which is 10x it's actual value.

Note: Chainlink oracles are used a just one piece of the OracleAggregator system and it is assumed that using a combination of other oracles, a scenario like this can be avoided. However this is not the case because the other oracles also have their flaws that can still allow this to be exploited. As an example if the chainlink oracle is being used with a UniswapV3Oracle which uses a long TWAP then this will be exploitable when the TWAP is near the minPrice on the way down. In a scenario like that it wouldn't matter what the third oracle was because it would be bypassed with the two matching oracles prices. If secondary oracles like Band are used a malicious user could DDOS relayers to prevent update pricing. Once the price becomes stale the chainlink oracle would be the only oracle left and it's price would be used.

Impact

In the event that an asset crashes (i.e. LUNA) the protocol can be manipulated to give out loans at an inflated price

Code Snippet

https://github.com/sherlock-audit/2023-02-blueberry/blob/main/contracts/oracle/ChainlinkAdapterOracle.sol#L66-L84

Tool used

Manual Review

Recommendation

ChainlinkAdapterOracle should check the returned answer against the minPrice/maxPrice and revert if the answer is outside of the bounds:

```
    (, int256 answer, , uint256 updatedAt, ) = registry.latestRoundData(
        token,
        USD
    );

+   if (answer >= maxPrice or answer <= minPrice) revert();
```

Discussion

Gornutz

The aggregator is responding with answers from the multiple of oracle sources

IAm0x52

Escalate for 50 USDC

This is not a dupe of #94

> The aggregator is responding with answers from the multiple of oracle sources

This comment is true but in my submission I address this exact issue and why it's still an issue even if the aggregator has multiple sources:

> Note: Chainlink oracles are used a just one piece of the OracleAggregator system and it is assumed that using a combination of other oracles, a scenario like this can be avoided. However this is not the case because the other oracles also have their flaws that can still allow this to be exploited. As an example if the chainlink oracle is being used with a UniswapV3Oracle which uses a long TWAP then this will be exploitable when the TWAP is near the minPrice on the way down. In a scenario like that it wouldn't matter what the third oracle was because it would be bypassed with the two matching oracles prices. If secondary oracles like Band are used a malicious user could DDOS relayers to prevent update pricing. Once the price becomes stale the chainlink oracle would be the only oracle left and it's price would be used.“‘

Even with the structure of aggregator there are still lots of scenarios where this could cause an issue. The chainlink oracle needs to revert at min/max answer because otherwise it risk returning the wrong price and causing the collateral to be overvalued leading to huge amounts of abuse.

sherlock-admin

> Escalate for 50 USDC
>
> This is not a dupe of #94
>
> `The aggregator is responding with answers from the multiple of oracle sources`
>
> This comment is true but in my submission I address this exact issue and why it's still an issue even if the aggregator has multiple sources:
>
> > Note: Chainlink oracles are used a just one piece of the OracleAggregator system and it is assumed that using a combination of other oracles, a scenario like this can be avoided. However this is not the case because the other oracles also have their flaws that can still allow this to be exploited. As an example if the chainlink oracle is being used with a UniswapV3Oracle which uses a long TWAP then this will be exploitable when the TWAP is near the minPrice on the way down. In a scenario like that it wouldn't matter what the third oracle was because it would be bypassed with the two matching oracles prices. If secondary oracles like Band are used a malicious user could DDOS relayers to prevent update pricing. Once the price becomes stale the chainlink oracle would be the only oracle left and it's price would be used.‘‘‘
>
> Even with the structure of aggregator there are still lots of scenarios where this could cause an issue. The chainlink oracle needs to revert at min/max answer because otherwise it risk returning the wrong price and causing the collateral to be overvalued leading to huge amounts of abuse.

You've created a valid escalation for 50 USDC!

To remove the escalation from consideration: Delete your comment. To change the amount you've staked on this escalation: Edit your comment **(do not create a new comment)**.

You may delete or edit your escalation comment anytime before the 48-hour escalation window closes. After that, the escalation becomes final.

Gornutz

Given the multi-aggregator setup we will use, once price hits Chainlink's oracles will at their min value. The other oracles will respond with a price well below that min value and will have a large enough deviation to cause a revert. Since the assets will be pooling from Chainlink / Band / Twap. Think setting a min / max inside of the chainlink oracle directly will potentially cause additional attack vectors to be created.

hrishibhat

Escalation accepted

Not a duplicate of #94 This issue is a valid medium Given the unlikely edge case of Chainlink hitting minimum value as a result of a serious price movement and resulting in undercollateralized borrowing.

sherlock-admin

> Escalation accepted
>
> This issue is a valid medium Given the unlikely edge case of Chainlink hitting minimum value as a result of a serious price movement and resulting in undercollateralized borrowing.

This issue's escalations have been accepted!

Contestants' payouts and scores will be updated according to the changes made on this issue.

Issue M-17: WIchiFarm will break after second deposit of LP

Source: https://github.com/sherlock-audit/2023-02-blueberry-judging/issues/15

Found by

0x52

Summary

WIchiFarm.sol makes the incorrect assumption that IchiVaultLP doesn't reduce allowance when using the transferFrom if allowance is set to type(uint256).max. Looking at a currently deployed IchiVault this assumption is not true. On the second deposit for the LP token, the call will always revert at the safe approve call.

Vulnerability Detail

IchiVault

```
function transferFrom(address sender, address recipient, uint256 amount) public
↪  virtual override returns (bool) {
    _transfer(sender, recipient, amount);
    _approve(sender, _msgSender(), _allowances[sender][_msgSender()].sub(amount,
    ↪  "ERC20: transfer amount exceeds allowance"));
    return true;
}
```

The above lines show the trasnferFrom call which reduces the allowance of the spender regardless of whether the spender is approved for type(uint256).max or not.

```
if (
    IERC20Upgradeable(lpToken).allowance(
        address(this),
        address(ichiFarm)
    ) != type(uint256).max
) {
    // We only need to do this once per pool, as LP token's allowance won't
    ↪  decrease if it's -1.
    IERC20Upgradeable(lpToken).safeApprove(
        address(ichiFarm),
        type(uint256).max
    );
}
```

As a result after the first deposit the allowance will be less than type(uint256).max. When there is a second deposit, the reduced allowance will trigger a safeApprove call.

```
function safeApprove(
    IERC20Upgradeable token,
    address spender,
    uint256 value
) internal {
    // safeApprove should only be called when setting an initial allowance,
    // or when resetting it to zero. To increase and decrease it, use
    // 'safeIncreaseAllowance' and 'safeDecreaseAllowance'
    require(
        (value == 0) || (token.allowance(address(this), spender) == 0),
        "SafeERC20: approve from non-zero to non-zero allowance"
    );
    _callOptionalReturn(token, abi.encodeWithSelector(token.approve.selector,
    ↪  spender, value));
}
```

safeApprove requires that either the input is zero or the current allowance is zero. Since neither is true the call will revert. The result of this is that WIchiFarm is effectively broken after the first deposit.

Impact

WIchiFarm is broken and won't be able to process deposits after the first.

Code Snippet

https://github.com/sherlock-audit/2023-02-blueberry/blob/main/contracts/wrapper/WIchiFarm.sol#L38

Tool used

Manual Review

Recommendation

Only approve is current allowance isn't enough for call. Optionally add zero approval before the approve. Realistically it's impossible to use the entire type(uint256).max, but to cover edge cases you may want to add it.

```
    if (
        IERC20Upgradeable(lpToken).allowance(
            address(this),
```

```
            address(ichiFarm)
-       ) != type(uint256).max
+       ) < amount
    ) {

+       IERC20Upgradeable(lpToken).safeApprove(
+           address(ichiFarm),
+           0
        );
        // We only need to do this once per pool, as LP token's allowance won't
        ↪  decrease if it's -1.
        IERC20Upgradeable(lpToken).safeApprove(
            address(ichiFarm),
            type(uint256).max
        );
    }
```

Discussion

SergeKireev

Escalate for 31 USDC

The impact stated is medium, since it only prevents additional deposits and no funds are at risk. The high severity definition as stated per Sherlock docs:

> This vulnerability would result in a material loss of funds and the cost of the attack is low (relative to the amount of funds lost). The attack path is possible with reasonable assumptions that mimic on-chain conditions. The vulnerability must be something that is not considered an acceptable risk by a reasonable protocol team.

sherlock-admin

> Escalate for 31 USDC
>
> The impact stated is medium, since it only prevents additional deposits and no funds are at risk. The high severity definition as stated per Sherlock docs:
>
> > This vulnerability would result in a material loss of funds and the cost of the attack is low (relative to the amount of funds lost). The attack path is possible with reasonable assumptions that mimic on-chain conditions. The vulnerability must be something that is not considered an acceptable risk by a reasonable protocol team.

You've created a valid escalation for 31 USDC!

To remove the escalation from consideration: Delete your comment. To change the amount you've staked on this escalation: Edit your comment **(do not create a new comment)**.

You may delete or edit your escalation comment anytime before the 48-hour escalation window closes. After that, the escalation becomes final.

hrishibhat

Escalation accepted

As the impact is only preventing further deposits rendering the farm contract useless, without causing a loss of funds.

sherlock-admin

> Escalation accepted
>
> As the impact is only preventing further deposits rendering the farm contract useless, without causing a loss of funds.

This issue's escalations have been accepted!

Contestants' payouts and scores will be updated according to the changes made on this issue.

Issue M-18: ChainlinkAdapterOracle use BTC/USD chainlink oracle to price WBTC which is problematic if WBTC depegs

Source: https://github.com/sherlock-audit/2023-02-blueberry-judging/issues/9

Found by

0x52

Summary

The chainlink BTC/USD oracle is used to price WBTC (docs). WBTC is basically a bridged asset and if the bridge is compromised/fails then WBTC will depeg and will no longer be equivalent to BTC. This will lead to large amounts of borrowing against an asset that is now effectively worthless. Since the protocol still values it via BTC/USD the protocol will not only be stuck with the bad debt caused by the currently outstanding loans but they will also continue to give out bad loans and increase the amount of bad debt further

Vulnerability Detail

See summary.

Impact

Protocol will take on a large amount of bad debt should WBTC bridge become compromised and WBTC depegs

Code Snippet

https://github.com/sherlock-audit/2023-02-blueberry/blob/main/contracts/oracle/ChainlinkAdapterOracle.sol#L47-L59

Tool used

Manual Review

Recommendation

I would recommend using a double oracle setup. Use both the Chainlink and another on-chain liquidity base oracle (i.e. UniV3 TWAP). If the price of the on-chain liquidity oracle drops below a certain threshold of the Chainlink oracles (i.e. 2% lower), any borrowing should be immediately halted. The chainlink oracle

will prevent price manipulation and the liquidity oracle will safeguard against the asset depegging.