SHERLOCK

SHERLOCK SECURITY REVIEW FOR

SHERLOCK

Prepared for:	bullvbear
Prepared by:	Sherlock
Lead Security Expert:	WATCHPUG
Dates Audited:	November 14 - November 17, 2022
Prepared on:	November 30, 2022

Introduction

With Bull v Bear you can short NFT collections, hedge your portfolio and buy discounted NFTs. Soon, on Ethereum.

Scope

`src/BvbProtocol.sol`

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
2	4

Issues not fixed or acknowledged

Medium	High
0	0

Security experts who found valid issues

ak1
WATCHPUG
KingNFT
Bahurum
carrot
bin2chen
ElKu
kirk-baird
hansfriese
GimelSec
neumo
0x52
Ruhum
Zarf
__141345__
0x4non
0xSmartContract
rvierdiiev
dipp
aviggiano
curiousapple
imare
cccz
obront

SHERLOCK

0xmuxyz
0xadrii
0v3rf10w
Tomo
tives
pashov

Issue H-1: Attackers can use `reclaimContract()` to transfer assets in protocol to address(0)

Source: https://github.com/sherlock-audit/2022-11-bullvbear-judging/issues/127

Found by

GimelSec, bin2chen, Ruhum, kirk-baird, __141345__, 0x52, carrot, hansfriese

Summary

`reclaimContract()` would transfer payment tokens to `bulls[contractId]`. An attacker can make `reclaimContract()` transfer assets to address(0).

Vulnerability Detail

An attacker can use a fake order to trick `reclaimContract()`. The fake order needs to meet the following requirements:

- `block.timestamp>order.expiry`.
- `!settledContracts[contractId]`.
- `!reclaimedContracts[contractId],`.

The first one is easy to fulfilled, an attacker can decide the content of the fake order. And the others are all satisfied since the fake order couldn't be settled or reclaimed before.

Thus, `reclaimContract()` would run this line: `IERC20(order.asset).safeTransfer(bull,bullAssetAmount);`. `bull` is address(0) since `bulls[contractId]` hasn't been filled. If `order.asset`'s implementation doesn't make sure `to!=address(0)`(e.g., https://github.com/ConsenSys/Tokens/blob/fdf687c69d998266a95f15216b1955a4965a0a6d/contracts/eip20/EIP20.sol). The asset would be sent to address(0).

```
function reclaimContract(Order calldata order) public nonReentrant {
    bytes32 orderHash = hashOrder(order);

    // ContractId
    uint contractId = uint(orderHash);

    address bull = bulls[contractId];

    // Check that the contract is expired
    require(block.timestamp > order.expiry, "NOT_EXPIRED_CONTRACT");

    // Check that the contract is not settled
```


SHERLOCK

```
    require(!settledContracts[contractId], "SETTLED_CONTRACT");

    // Check that the contract is not reclaimed
    require(!reclaimedContracts[contractId], "RECLAIMED_CONTRACT");

    uint bullAssetAmount = order.premium + order.collateral;
    if (bullAssetAmount > 0) {
        // Transfer payment tokens to the Bull
        IERC20(order.asset).safeTransfer(bull, bullAssetAmount);
    }

    reclaimedContracts[contractId] = true;

    emit ReclaimedContract(orderHash, order);
}
```

Impact

An attacker can use this vulnerability to transfer assets from BvB to address(0). It results in serious loss of funds.

Code Snippet

https://github.com/sherlock-audit/2022-11-bullvbear/blob/main/bvb-protocol/src/BvbProtocol.sol#L417-L443

Tool used

Manual Review

Recommendation

There are multiple solutions for this problem.

1. check `bulls[contractId]!=address(0)`
2. check the order is matched `matchedOrders[contractId].maker!=address(0)`

Discussion

datschill

PR fixing this issue : https://github.com/BullvBear/bvb-solidity/pull/4

Issue H-2: Bull can `transferPosition()` to `address(0)` and the original order can be matched again

Source: https://github.com/sherlock-audit/2022-11-bullvbear-judging/issues/114

Found by

GimelSec, dipp, aviggiano, Bahurum, bin2chen, curiousapple, imare, KingNFT, rvierdiiev, 0x52, carrot, hansfriese, WATCHPUG, neumo

Summary

Using `bulls[uint(orderHash)]==address(0)` to check whether the order is matched is insufficient, the bull can `transferPosition` to `address(0)` and the order can be matched again.

Vulnerability Detail

An order must not be matched more than once.

There is a check presented in the current implementation to prevent that: L760 `require(bulls[uint(orderHash)]==address(0),"ORDER_ALREADY_MATCHED");`.

However, this check can be easily bypassed by the bull, as they can `transferPosition()` to `address(0)` anytime.

Then the original order can be matched again.

Impact

Attacker can match the orders by bear makers multiple times, pulling `order.premium+bearFees` from the victims' wallet as many times as they want.

Code Snippet

https://github.com/sherlock-audit/2022-11-bullvbear/blob/main/bvb-protocol/src/BvbProtocol.sol#L734-L761

https://github.com/sherlock-audit/2022-11-bullvbear/blob/main/bvb-protocol/src/BvbProtocol.sol#L521-L538

Tool used

Manual Review

Recommendation

Consider using `matchedOrders[contractId]` to check if the order has been matched or not. Also, consider disallowing `transferPosition()` to `address(0)`.

Discussion

datschill

PR fixing this issue : https://github.com/BullvBear/bvb-solidity/pull/1

datschill

PR fixing the transfer to 0x0 : https://github.com/BullvBear/bvb-solidity/pull/3

Issue H-3: Bull can prevent `settleContract()`

Source: https://github.com/sherlock-audit/2022-11-bullvbear-judging/issues/111

Found by

Bahurum, KingNFT, ak1, ElKu, WATCHPUG

Summary

The bull can intentionally cause out-of-gas and revert the transaction and prevent `settleContract()`.

Vulnerability Detail

As `IERC721(order.collection).safeTransferFrom()` is used in `settleContract()` which will call `IERC721Receiver(to).onERC721Received()` when the `to` address is an contract.

This gives the bull a chance to intentionally prevent the transaction from happening by consuming a lot of gas and revert the whole transaction.

Impact

The bear (victim) can not `settleContract()` therefore cannot exercise their put option rights. The bull (attacker) always wins.

Code Snippet

https://github.com/sherlock-audit/2022-11-bullvbear/blob/main/bvb-protocol/src/BvbProtocol.sol#L374-L411

Tool used

Manual Review

Recommendation

```
function settleContract(Order calldata order, uint tokenId) public nonReentrant {
    bytes32 orderHash = hashOrder(order);

    // ContractId
    uint contractId = uint(orderHash);

    address bear = bears[contractId];
```


SHERLOCK

```
    // Check that only the bear can settle the contract
    require(msg.sender == bear, "ONLY_BEAR");

    // Check that the contract is not expired
    require(block.timestamp < order.expiry, "EXPIRED_CONTRACT");

    // Check that the contract is not already settled
    require(!settledContracts[contractId], "SETTLED_CONTRACT");

    address bull = bulls[contractId];

-    // Try to transfer the NFT to the bull (needed in case of a malicious bull
↪   that block transfers)
-    try IERC721(order.collection).safeTransferFrom(bear, bull, tokenId) {}
-    catch (bytes memory) {
        // Transfer NFT to BvbProtocol
        IERC721(order.collection).safeTransferFrom(bear, address(this), tokenId);
        // Store that the bull has to retrieve it
        withdrawableCollectionTokenId[order.collection][tokenId] = bull;
-    }

    uint bearAssetAmount = order.premium + order.collateral;
    if (bearAssetAmount > 0) {
        // Transfer payment tokens to the Bear
        IERC20(order.asset).safeTransfer(bear, bearAssetAmount);
    }

    settledContracts[contractId] = true;

    emit SettledContract(orderHash, tokenId, order);
}
```

Discussion

datschill

PR fixing this issue : https://github.com/BullvBear/bvb-solidity/pull/14

Issue H-4: Reentrancy in `withdrawToken()` May Delete The Next User's Balance

Source: https://github.com/sherlock-audit/2022-11-bullvbear-judging/issues/88

Found by

bin2chen, 0x4non, kirk-baird, Zarf, ak1, 0xSmartContract, carrot, neumo

Summary

The function `withdrawToken()` does not have a reentrancy guard and calls an external contract. It is possible to reenter `settleContract()` to spend the same token that was just transferred out. If the `safeTransferFrom()` in `settleContract()` fails then the token balance is added to the bull. However, when `withdrawToken()` continues execution it will delete the balance of the bull.

Vulnerability Detail

`withdrawToken()` makes a state change to `withdrawableCollectionTokenId[collection][tokenId]` after it makes an external call to an ERC721 contract `safeTransferFrom()`. Since this external call will relinquish control to the `to` address which is `recipient`, the `recipient` smart contract may reenter `settleContract()`.

When calling `settleContract()` set the `tokenId` function parameter to the same one just transferred in `withdawToken()`. If transfer to the `bull` fails then the token is instead transferred to `BvbProtocol` and balance added to the bull, `withdrawableCollectionTokenId[order.collection][tokenId]=bull`

After `settleContract()` finishes executing control will revert back to `withdrawToken()` which then executes the line `withdrawableCollectionTokenId[collection][tokenId]=address(0)`. The balance of the bull is therefore delete for that token.

e.g. If we know a transfer will fail to a bull in a matched order we can a) create a fake order with ourselves b) reenter from `withdrawToken()` into `settleContract()` and therefore delete the bulls `withdrawableCollectionTokenId` balance. Steps:

- `BvpProtocol.matchOrder(orderA)` create a fake order (A) with ones self
- `BvpProtocol.settleOrder(orderA)` settle the fake order (A) with ones self and ensure the ERC721 transfer from bull to bear fails.
- `BvpProtocol.matchOrder(orderB)` match the real order (B), this can be done at any time
- `BvbProtocol.withdrawToken(orderA,token1)` the following setups happen during line #456

SHERLOCK

  - `ERC721(collection).safeTransferFrom(this,recipient,tokenId)` (`recipient` is bull from the fake order (A))
  - `recipient.onERC721Received()` called by `safeTransferFrom()` and gives execution control to `receipient`
  - `BvpProtocol.settleOrder(orderB,token1)` reenter to settle the real order using `token1` which does `withdrawableCollectionTokenId[order.collection][tokenId]=bull`
- Finish executing `BvbProtocol.withdrawToken(orderA,token1)` after line #456 which does `withdrawableCollectionTokenId[collection][tokenId]=address(0)`

Impact

If we know a transfer is going to fail to a `bull` for an ERC721 we can ensure the NFT is locked in the `BvbProtocol` contract. This NFT will be unrecoverable.

Code Snippet

withdrawToken()

```
function withdrawToken(bytes32 orderHash, uint tokenId) public {
    address collection = matchedOrders[uint(orderHash)].collection;

    address recipient = withdrawableCollectionTokenId[collection][tokenId];

    // Transfer NFT to recipient
    IERC721(collection).safeTransferFrom(address(this), recipient, tokenId);

    // This token is not withdrawable anymore
    withdrawableCollectionTokenId[collection][tokenId] = address(0);
```

settleContract()

```
function settleContract(Order calldata order, uint tokenId) public nonReentrant {
    bytes32 orderHash = hashOrder(order);

    // ContractId
    uint contractId = uint(orderHash);

    address bear = bears[contractId];

    // Check that only the bear can settle the contract
    require(msg.sender == bear, "ONLY_BEAR");

    // Check that the contract is not expired
```

```
    require(block.timestamp < order.expiry, "EXPIRED_CONTRACT");

    // Check that the contract is not already settled
    require(!settledContracts[contractId], "SETTLED_CONTRACT");

    address bull = bulls[contractId];

    // Try to transfer the NFT to the bull (needed in case of a malicious bull
↪   that block transfers)
    try IERC721(order.collection).safeTransferFrom(bear, bull, tokenId) {}
    catch (bytes memory) {
        // Transfer NFT to BvbProtocol
        IERC721(order.collection).safeTransferFrom(bear, address(this), tokenId);
        // Store that the bull has to retrieve it
        withdrawableCollectionTokenId[order.collection][tokenId] = bull;
    }

    uint bearAssetAmount = order.premium + order.collateral;
    if (bearAssetAmount > 0) {
        // Transfer payment tokens to the Bear
        IERC20(order.asset).safeTransfer(bear, bearAssetAmount);
    }

    settledContracts[contractId] = true;

    emit SettledContract(orderHash, tokenId, order);
}
```

Tool used

Manual Review

Recommendation

I recommend both of these solutions though either one will be sufficient on its own:

- Add `nonReentrant` modifier to `withdrawToken()`
- Set `withdrawableCollectionTokenId[collection][tokenId]=address(0)` before performing `IERC721(collection).safeTransferFrom(address(this),recipient, tokenId)` to apply the checks-effects-interactions pattern.

Discussion

datschill

PR fixing checks-effects-interactions pattern :
https://github.com/BullvBear/bvb-solidity/pull/15

datschill

PR fixing another issue, removing the withdrawToken() method :
https://github.com/BullvBear/bvb-solidity/pull/14

Issue M-1: It doesn't handle fee-on-transfer/deflationary tokens

Source: https://github.com/sherlock-audit/2022-11-bullvbear-judging/issues/130

Found by

GimelSec, dipp, tives, Ruhum, rvierdiiev, cccz, Zarf, 0v3rf10w, Tomo, hansfriese, pashov

Summary

The protocol doesn't handle fee-on-transfer/deflationary tokens, users will be unable to call `settleContract` and `reclaimContract` due to not enough assets in the contract. Though the protocol uses `allowedAsset` to set the asset as supported as payment, we can't guarantee that the allowed non-deflationary token will always not become a deflationary token, especially upgradeable tokens (for example, USDC).

Vulnerability Detail

Assume that A token is a deflationary token, and it will take 50% fee when transferring tokens. And the protocol only set 4% fee.

If a user is bear and call `mathOrder` with `order.premium=100`, the `takerPrice` will be `100+100*4%=104` but the protocol will only get `104*50%=52` tokens in L354. Same problem in `order.collateral`, the user will be unable to call `settleContract` because the contract doesn't have enough A tokens.

Impact

The protocol will be unable to pay enough tokens to users when users want to call `settleContract` or `reclaimContract`.

Code Snippet

https://github.com/sherlock-audit/2022-11-bullvbear/blob/main/bvb-protocol/src/BvbProtocol.sol#L354 https://github.com/sherlock-audit/2022-11-bullvbear/blob/main/bvb-protocol/src/BvbProtocol.sol#L358

Tool used

Manual Review

SHERLOCK

Recommendation

Use `balanceAfter-balanceBefore`:

```
uint256 balanceBefore = deflationaryToken.balanceOf(address(this));
deflationaryToken.safeTransferFrom(msg.sender, address(this), takerPrice);
uint256 balanceAfter = deflationaryToken.balanceOf(address(this));
premium = (balanceAfter - balanceBefore) - bearFees;
```

Discussion

datschill

PR fixing this issue : https://github.com/BullvBear/bvb-solidity/pull/8

Issue M-2: Bulls that are unable to receive NFTs will not be able to claim them later

Source: https://github.com/sherlock-audit/2022-11-bullvbear-judging/issues/4

Found by

GimelSec, bin2chen, 0xadrii, rvierdiiev, cccz, obront, 0xmuxyz, carrot, hansfriese, WATCHPUG

Summary

A lot of care has been taken to ensure that, if a bull has a contract address that doesn't accept ERC721s, the NFT is saved to `withdrawableCollectionTokenId` for later withdrawal. However, because there is no way to withdraw this token to a different address (and the original address doesn't accept NFTs), it will never be able to be claimed.

Vulnerability Detail

To settle a contract, the bear calls `settleContract()`, which sends their NFT to the bull, and withdraws the collateral and premium to the bear.

```
try IERC721(order.collection).safeTransferFrom(bear, bull, tokenId) {}
catch (bytes memory) {
    // Transfer NFT to BvbProtocol
    IERC721(order.collection).safeTransferFrom(bear, address(this), tokenId);
    // Store that the bull has to retrieve it
    withdrawableCollectionTokenId[order.collection][tokenId] = bull;
}

uint bearAssetAmount = order.premium + order.collateral;
if (bearAssetAmount > 0) {
    // Transfer payment tokens to the Bear
    IERC20(order.asset).safeTransfer(bear, bearAssetAmount);
}
```

In order to address the case that the bull is a contract that can't accept NFTs, the protocol uses a try-catch setup. If the transfer doesn't succeed, it transfers the NFT into the contract, and sets `withdrawableCollectionTokenId` so that the specific NFT is attributed to the bull for later withdrawal.

However, assuming the bull isn't an upgradeable contract, this withdrawal will never be possible, because their only option is to call the same function `safeTransferFrom` to the same contract address, which will fail in the same way.

```
function withdrawToken(bytes32 orderHash, uint tokenId) public {
    address collection = matchedOrders[uint(orderHash)].collection;

    address recipient = withdrawableCollectionTokenId[collection][tokenId];

    // Transfer NFT to recipient
    IERC721(collection).safeTransferFrom(address(this), recipient, tokenId);

    // This token is not withdrawable anymore
    withdrawableCollectionTokenId[collection][tokenId] = address(0);

    emit WithdrawnToken(orderHash, tokenId, recipient);
}
```

Impact

If a bull is a contract that can't receive NFTs, their orders will be matched, the bear will be able to withdraw their assets, but the bull's NFT will remain stuck in the BVB protocol contract.

Code Snippet

https://github.com/sherlock-audit/2022-11-bullvbear/blob/main/bvb-protocol/src/BvbProtocol.sol#L394-L406

https://github.com/sherlock-audit/2022-11-bullvbear/blob/main/bvb-protocol/src/BvbProtocol.sol#L450-L462

Tool used

Manual Review

Recommendation

There are a few possible solutions:

- Add a `to` field in the `withdrawToken` function, which allows the bull to withdraw the NFT to another address
- Create a function similar to `transferPosition` that can be used to transfer owners of a withdrawable NFT
- Decide that you want to punish bulls who aren't able to receive NFTs, in which case there is no need to save their address or implement a `withdrawToken` function

Discussion

datschill

PR fixing another issue, removing the withdrawToken() method : https://github.com/BullvBear/bvb-solidity/pull/14

datschill

This issue isn't High, because in the default behavior, no smart contract can match an Order. So for a Bull to be a smart contract, the user needs to match an order (as a maker or a taker) with an EOA, then transfer his position to a smart contract. This would be kind of a poweruser move, so we consider that he should be aware that his smart contract should handle NFT reception. Whatsoever, the issue is fixed thanks to the PR#14, the user will be able to transfer his position to whatever EOA or smart contract he wants before calling reclaimContract() to retrieve ERC20 assets or ERC721.