Cyberscope

Audit Report

ShadowFi

April 2024

SHA256 2861de8e8d4a724a80e4a169b59e6b02f888a7d1d8de64b12853793b293abebc

SHA256 7670412595a6f66525494fbd1b1a71a2be9c11cd570d3b14a83cfeba55f5a944

Audited by © cyberscope

Table of Contents

Review

ShadowGold.sol	https://testnet.bscscan.com/address/0x1a24df2fb9e00b8e0736780f2ac93e6d207e7932
DividendDistributor.sol	https://testnet.bscscan.com/address/0xa94af93ab0263e23defcc94223ed8b830dab3b65

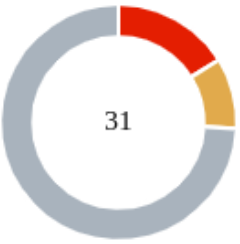
Audit Updates

Initial Audit	03 Apr 2024

Source Files

Filename	SHA256
ShadowGold.sol	2861de8e8d4a724a80e4a169b59e6b02f888a7d1d8de64b12853793b293abebc
DividendDistributor.sol	7670412595a6f66525494fbd1b1a71a2be9c11cd570d3b14a83cfeba55f5a944

Findings Breakdown



Critical	5
Medium	3
Minor / Informative	23

Severity	Unresolved	Acknowledged	Resolved	Other
Critical	5	0	0	0
Medium	3	0	0	0
Minor / Informative	23	0	0	0

Diagnostics

Critical Medium Minor / Informative

Severity	Code	Description	Status
●	ELFM	Exceeds Fees Limit	Unresolved
●	MT	Mints Tokens	Unresolved
●	ST	Stops Transactions	Unresolved
●	US	Untrusted Source	Unresolved
●	ZD	Zero Division	Unresolved
●	BC	Blacklists Addresses	Unresolved
●	CSD	Circulating Supply Discrepancy	Unresolved
●	UDB	Unupdated Distributor Balances	Unresolved
●	ALM	Array Length Mismatch	Unresolved
●	CO	Code Optimization	Unresolved
●	DDP	Decimal Division Precision	Unresolved
●	IDI	Immutable Declaration Improvement	Unresolved
●	IPA	Inconsistent Permissions Amount	Unresolved
●	MEM	Misleading Error Messages	Unresolved

●	MMN	Misleading Method Naming	Unresolved
●	MIV	Missing Index Verification	Unresolved
●	PAV	Pair Address Validation	Unresolved
●	PLPI	Potential Liquidity Provision Inadequacy	Unresolved
●	PVC	Price Volatility Concern	Unresolved
●	RFV	Redundant Fee Variable	Unresolved
●	RRS	Redundant Require Statement	Unresolved
●	RSML	Redundant SafeMath Library	Unresolved
●	OCTD	Transfers Contract's Tokens	Unresolved
●	L04	Conformance to Solidity Naming Conventions	Unresolved
●	L06	Missing Events Access Control	Unresolved
●	L07	Missing Events Arithmetic	Unresolved
●	L11	Unnecessary Boolean equality	Unresolved
●	L14	Uninitialized Variables in Local Scope	Unresolved
●	L16	Validate Variable Setters	Unresolved
●	L19	Stable Compiler Version	Unresolved
●	L20	Succeeded Transfer Check	Unresolved

ELFM - Exceeds Fees Limit

Criticality	Critical
Location	DividendDistributor.sol#L741
Status	Unresolved

Description

The contract owner has the authority to increase over the allowed limit of 25%. The owner may take advantage of it by calling the `setLaunchedAt` function of the token contract with any arbitrary number effectively modifying the result of the `checkLaunched` in order to return a high percentage fee value.

```
if (ISDG(_token).checkLaunched() + 1 >= block.number) {
    return feeDenominator.sub(1);
}
```

Recommendation

The contract could embody a check for the maximum acceptable value. The team should carefully manage the private keys of the owner's account. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the contract admin functions.

Temporary Solutions:

These measurements do not decrease the severity of the finding

- Introduce a time-locker mechanism with a reasonable delay.
- Introduce a multi-signature wallet so that many addresses will confirm the action.
- Introduce a governance model where users will vote about the actions.

Permanent Solution:

- Renouncing the ownership, which will eliminate the threats but it is non-reversible.

MT - Mints Tokens

Criticality	Critical
Location	ShadowGold.sol#L714
Status	Unresolved

Description

he contract allows the owner to change and designate any address as the distributor via the `setDistributorAndFeeReceiverContract` function. This grants the owner unchecked authority to manipulate the distribution mechanism, by calling the `processFee` function to mint tokens to the `distributor` address. As a result, the contract tokens will be highly inflated.

```
    function processFee(address sender, uint256 feeAmount) external {
        require(
            msg.sender == address(distributor),
            "Only Distributor can Process Fee."
        );
        _balances[address(distributor)] =
_balances[address(distributor)].add(
            feeAmount
        );
        emit Transfer(sender, address(distributor), feeAmount);
    }
```

Recommendation

The team should carefully manage the private keys of the owner's account. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the contract admin functions.

Temporary Solutions:

These measurements do not decrease the severity of the finding

- Introduce a time-locker mechanism with a reasonable delay.
- Introduce a multi-signature wallet so that many addresses will confirm the action.

- Introduce a governance model where users will vote about the actions.

Permanent Solution:

- Renouncing the ownership, which will eliminate the threats but it is non-reversible.

ST - Stops Transactions

Criticality	Critical
Location	ShadowGold.sol#L628
Status	Unresolved

Description

The transactions are initially disabled for all users excluding the authorized addresses. The owner can enable the transactions for all users. Once the transactions are enable the owner will not be able to disable them again.

```
if (!allowedAddresses[msg.sender] && !allowedAddresses[recipient]) {
    require(
        block.timestamp > transferBlockTime,
        "Transfers have not been enabled yet."
    );
```

Additionally, the contract owner has the authority to stop transactions, as described in detail in sections `US` , and `ZD` . As a result, the contract might operate as a honeypot.

Recommendation

The team should carefully manage the private keys of the owner's account. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the contract admin functions. Some suggestions are:

- Introduce a multi-sign wallet so that many addresses will confirm the action.
- Introduce a governance model where users will vote about the actions.

US - Untrusted Source

Criticality	Critical
Location	ShadowGold.sol#L784
Status	Unresolved

Description

The contract uses an external contract in order to determine the transaction's flow. The external contract is untrusted. As a result, it may produce security issues and harm the transactions.

```
function setDistributorAndFeeReceiverContract(
    address _distributorContract,
    address _feeReceiver
) public onlyOwner {
    distributor = IDividendDistributor(_distributorContract);
    isDividendExempt[_distributorContract] = true;
    isFeeExempt[_feeReceiver] = true;
}
```

Recommendation

The contract should use a trusted external source. A trusted source could be either a commonly recognized or an audited contract. The pointing addresses should not be able to change after the initialization.

ZD - Zero Division

Criticality	Critical
Location	DividendDistributor.sol#L774,814,898
Status	Unresolved

Description

The contract is using variables that may be set to zero as denominators. This can lead to unpredictable and potentially harmful results, such as a transaction revert.

Specifically the `feeDenominator` , `buybackMultiplierDenominator` and `totalBuyFee` variables can be set to zero.

```
        uint256 feeAmount =
amount.mul(getTotalFee(isSell(recipient))).div(
            feeDenominator
         ...
         uint256 feeIncrease = totalFee
             .mul(buybackMultiplierNumerator)
             .div(buybackMultiplierDenominator)
             .sub(totalFee);
         ...
         uint256 swapAmount =
swapThreshold.mul(marketingFee).div(totalBuyFee);
```

Recommendation

It is important to handle division by zero appropriately in the code to avoid unintended behavior and to ensure the reliability and safety of the contract. The contract should ensure that the divisor is always non-zero before performing a division operation. It should prevent the variables to be set to zero, or should not allow the execution of the corresponding statements.

BC - Blacklists Addresses

Criticality	Medium
Location	ShadowGold.sol#L635
Status	Unresolved

Description

The contract owner has the authority to stop addresses from transactions. The owner may take advantage of it by calling the `blacklistAddress` function.

```
require(
    !blackList[sender] && !blackList[recipient],
    "Either the spender or recipient is blacklisted."
);
```

Recommendation

The team should carefully manage the private keys of the owner's account. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the contract admin functions.

Temporary Solutions:

These measurements do not decrease the severity of the finding

- Introduce a time-locker mechanism with a reasonable delay.
- Introduce a multi-signature wallet so that many addresses will confirm the action.
- Introduce a governance model where users will vote about the actions.

Permanent Solution:

- Renouncing the ownership, which will eliminate the threats but it is non-reversible.

CSD - Circulating Supply Discrepancy

Criticality	Medium
Location	ShadowGold.sol#L550
Status	Unresolved

Description

According to the ERC20 specification, the `totalSupply()` function should return the total supply of the token. The total supply should always equal the sum of the balances. The contract does not return the `totalSupply()`. Instead, the function returns the `totalSupply()` minus the amount that has been moved to the dead address. This amount is the circulating supply of the token. Many decentralized applications and tools are calculating many indicators like the circulating supply and market cap based on the `totalSupply()`. As a result, these applications will produce misleading results.

```
    function totalSupply() external view override returns (uint256) {
        return _totalSupply.sub(balanceOf(DEAD)).sub(balanceOf(ZERO));
    }
```

Recommendation

The `totalSupply()` should always equal the sum of the holder's balances. The contract should comply with this convention so that the decentralized applications will produce correct results.

UDB - Unupdated Distributor Balances

Criticality	Medium
Location	ShadowGold.sol#L640
Status	Unresolved

Description

The contract contains the `_transferFrom` which immediately executes the `_basicTransfer` function in case the `if` condition condition is met, resulting in a transfer transaction before updating the balances of the distributor. Consequently, the updated balances will not be reflected accurately in the distribution contract, leading to discrepancies in token distribution.

```
    function _transferFrom(
         address sender,
         address recipient,
         uint256 amount
     ) internal returns (bool) {
     ...

     if (IDividendDistributor(distributor).checkInSwap()) {
          return _basicTransfer(sender, recipient, amount);
      }
     ...
```

Recommendation

It is recommended to ensure that balances of the distributor are updated before executing any transfer transactions. Implement mechanisms to update the distributor balances synchronously with token transfers to maintain consistency in token distribution.

ALM - Array Length Mismatch

Criticality	Minor / Informative
Location	ShadowGold.sol#L893
Status	Unresolved

Description

The contract is designed to handle the process of elements from arrays through functions that accept multiple arrays as input parameters. These functions are intended to iterate over the arrays, processing elements from each array in a coordinated manner. However, there are no explicit checks to verify that the lengths of these input arrays are equal. This lack of validation could lead to scenarios where the arrays have differing lengths, potentially causing out-of-bounds access if the function attempts to process beyond the end of the shorter array. Such situations could result in unexpected behavior or errors during the contract's execution, compromising its reliability and security.

```
    function airdrops(
        address[] memory _users,
        uint256[] memory _amounts
    ) external onlyOwner {
        for (uint8 i = 0; i < _users.length; i++) {
            airdrop(_users[i], _amounts[i]);
        }
    }
```

Recommendation

To mitigate this, it is recommended to incorporate a validation check at the beginning of the function that accepts multiple arrays to ensure that the lengths of these arrays are identical. This can be achieved by implementing a conditional statement that compares the lengths of the arrays, and reverts the transaction if the lengths do not match. Such a validation step will prevent out-of-bounds errors and ensure that elements from each array are processed in a paired and coordinated manner, thus preserving the integrity and intended functionality of the contract.

CO - Code Optimization

Criticality	Minor / Informative
Location	DividendDistributor.sol#L783
Status	Unresolved

Description

There are code segments that could be optimized. A segment may be optimized so that it becomes a smaller size, consumes less memory, executes more rapidly, or performs fewer operations. Specifically the `isSell` function could directly return the result of the `isPair(recipient)` function without the conditional check, thereby optimizing code efficiency.

```
    function isSell(address recipient) internal view returns (bool) {
        if (isPair(recipient)) return true;
        return false;
    }
```

Recommendation

The team is advised to take these segments into consideration and rewrite them so the runtime will be more performant. That way it will improve the efficiency and performance of the source code and reduce the cost of executing it. It is recommended to simplify the isSell function by directly returning the result of the `isPair(recipient)` function.

DDP - Decimal Division Precision

Criticality	Minor / Informative
Location	DividendDistributor.sol#L919
Status	Unresolved

Description

Division of decimal (fixed point) numbers can result in rounding errors due to the way that division is implemented in Solidity. Thus, it may produce issues with precise calculations with decimal numbers.

Solidity represents decimal numbers as integers, with the decimal point implied by the number of decimal places specified in the type (e.g. decimal with 18 decimal places). When a division is performed with decimal numbers, the result is also represented as an integer, with the decimal point implied by the number of decimal places in the type. This can lead to rounding errors, as the result may not be able to be accurately represented as an integer with the specified number of decimal places.

Hence, the splitted shares will not have the exact precision and some funds may not be calculated as expected.

```
uint256 swapAmount = swapThreshold.mul(marketingFee).div(totalBuyFee);
...
uint256 amountSDGReflection = swapThreshold.mul(reflectionFee).div(
    totalBuyFee
);
uint256 amountSDGReceiver = swapThreshold.mul(sdgReceiverFee).div(
    totalBuyFee
);
uint256 amountSDGBuyback = swapThreshold.mul(buybackFee).div(
    totalBuyFee
```

Recommendation

The team is advised to take into consideration the rounding results that are produced from the solidity calculations. The contract could calculate the subtraction of the divided funds in the last calculation in order to avoid the division rounding issue.

IDI - Immutable Declaration Improvement

Criticality	Minor / Informative
Location	ShadowGold.sol#L519,523
Status	Unresolved

Description

The contract declares state variables that their value is initialized once in the constructor and are not modified afterwards. The `immutable` is a special declaration for this kind of state variables that saves gas when it is defined.

```
wethPair
paxgPair
```

Recommendation

By declaring a variable as immutable, the Solidity compiler is able to make certain optimizations. This can reduce the amount of storage and computation required by the contract, and make it more gas-efficient.

IPA - Inconsistent Permissions Amount

Criticality	Minor / Informative
Location	ShadowGold.sol#L188
Status	Unresolved

Description

The contract is initialized with the constant `NUM_PERMISSIONS` variable set to 10. However, the total number of permissions defined within the contract amounts to 7. This inconsistency between the declared number of permissions and the actual count poses a potential risk to the integrity and functionality of the smart contract.

```
   uint256 constant NUM_PERMISSIONS = 10; // always has to be adjusted
when Permission element is added or removed
...
permissionNameToIndex["ChangeFees"] = uint256(Permission.ChangeFees);
permissionNameToIndex["Buyback"] = uint256(Permission.Buyback);
permissionNameToIndex["AdjustContractVariables"] = uint256(
    Permission.AdjustContractVariables
);
permissionNameToIndex["Authorize"] = uint256(Permission.Authorize);
permissionNameToIndex["Unauthorize"] = uint256(Permission.Unauthorize);
permissionNameToIndex["LockPermissions"] = uint256(
    Permission.LockPermissions
);
permissionNameToIndex["ExcludeInclude"] = uint256(
    Permission.ExcludeInclude
);
```

Recommendation

It is recommended to ensure alignment between the declared `NUM_PERMISSIONS` constant variable and the actual number of permissions defined within the contract. This can be achieved by either adjusting the `NUM_PERMISSIONS` constant to accurately reflect the total permissions or by adding the necessary permissions to match the declared constant. Regularly reviewing and updating this alignment during code modifications is also advised to maintain consistency and prevent potential errors or vulnerabilities.

MEM - Misleading Error Messages

Criticality	Minor / Informative
Location	ShadowGold.sol#L659,796,803,840 DividendDistributor.sol#L523,529,812
Status	Unresolved

Description

The contract is using misleading error messages. These error messages do not accurately reflect the problem, making it difficult to identify and fix the issue. As a result, the users will not be able to find the root cause of the error.

```
require(_balances[sender] > 0)
require(amount >= _totalSupply / 2000)

require(
            (holder != address(this) && holder != wethPair) ||
                holder != paxgPair
        )
require(gas <= 1000000)
require(!initialized)
require(msg.sender == _token)
require(numerator / denominator <= 3 && numerator > denominator)
```

Recommendation

The team is suggested to provide a descriptive message to the errors. This message can be used to provide additional context about the error that occurred or to explain why the contract execution was halted. This can be useful for debugging and for providing more information to users that interact with the contract.

MMN - Misleading Method Naming

Criticality	Minor / Informative
Location	ShadowGold.sol#L845
Status	Unresolved

Description

Methods can have misleading names if their names do not accurately reflect the functionality they contain or the purpose they serve. The contract uses some method names that are too generic or do not clearly convey the underneath functionality. Misleading method names can lead to confusion, making the code more difficult to read and understand. Methods can have misleading names if their names do not accurately reflect the functionality they contain or the purpose they serve. The contract uses some method names that are too generic or do not clearly convey the underneath functionality. Misleading method names can lead to confusion, making the code more difficult to read and understand.

Specifically, the `getCirculatingSupply` function calculate the circulating supply but behaves similarly to `getMaxCirculatingSupply`, since this function subtracts the balance of a "DEAD" address and a "ZERO" address from the maximum supply, potentially providing misleading information about the actual circulating supply.

```
    function getCirculatingSupply() public view returns (uint256) {
        return _maxSupply.sub(balanceOf(DEAD)).sub(balanceOf(ZERO));
    }
```

Recommendation

It's always a good practice for the contract to contain method names that are specific and descriptive. The team is advised to keep in mind the readability of the code. It is recommended to revise the `getCirculatingSupply` function to accurately reflect the circulating supply by excluding addresses that are not actively participating in the circulation from the total supply.

MIV - Missing Index Verification

Criticality	Minor / Informative
Location	ShadowGold.sol#L272,286,300
Status	Unresolved

Description

The contract contains the `authorizeForMultiplePermissions`, `unauthorizeFor`, and `unauthorizeForMultiplePermissions` functions, all relying on `permIndex` for permission handling. However, these functions lack verification to ensure the existence of the `permIndex` before its usage. Consequently, users could define a `permIndex` that does not exist, leading to potential unauthorized access or unintended behavior.

```
    function authorizeForMultiplePermissions(
        address adr,
        string[] calldata permissionNames
    ) public authorizedFor(Permission.Authorize) {
        for (uint256 i; i < permissionNames.length; i++) {
            uint256 permIndex =
permissionNameToIndex[permissionNames[i]];
            authorizations[adr][permIndex] = true;
            emit AuthorizedFor(adr, permissionNames[i], permIndex);
        }
    }

    function unauthorizeFor(
        address adr,
        string memory permissionName
    ) public authorizedFor(Permission.Unauthorize) {
        require(adr != owner, "Can't unauthorize owner");

        uint256 permIndex = permissionNameToIndex[permissionName];
        authorizations[adr][permIndex] = false;
        emit UnauthorizedFor(adr, permissionName, permIndex);
    }

    function unauthorizeForMultiplePermissions(
        address adr,
        string[] calldata permissionNames
    ) public authorizedFor(Permission.Unauthorize) {
        require(adr != owner, "Can't unauthorize owner");

        for (uint256 i; i < permissionNames.length; i++) {
            uint256 permIndex =
permissionNameToIndex[permissionNames[i]];
            authorizations[adr][permIndex] = false;
            emit UnauthorizedFor(adr, permissionNames[i], permIndex);
        }
    }
```

Recommendation

It is recommended to enhance the functions by incorporating additional checks to validate the existence of the `permIndex` before executing operations. This would mitigate the risk of unauthorized access and ensure the contract behaves as intended.

PAV - Pair Address Validation

Criticality	Minor / Informative
Location	DividendDistributor.sol#L633,819,843
Status	Unresolved

Description

The contract is missing address validation in the pair address argument. The absence of validation reveals a potential vulnerability, as it lacks proper checks to ensure the integrity and validity of the pair address provided as an argument. The pair address is a parameter used in certain methods of decentralized exchanges for functions like token swaps and liquidity provisions.

The absence of address validation in the pair address argument can introduce security risks and potential attacks. Without proper validation, if the owner's address is compromised, the contract may lead to unexpected behavior like loss of funds.

```
address[] memory path = new address[](2);
path[0] = address(_token);
path[1] = address(PAXG);
...
function buyTokensWETH(uint256 amount, address to) internal swapping {
    address[] memory path = new address[](2);
    path[0] = address(WETH);
    path[1] = address(_token);
    ...

function buyTokensPAXG(uint256 amount, address to) internal swapping {
    address[] memory path = new address[](2);
    path[0] = address(PAXG);
    path[1] = address(_token);
```

Recommendation

To mitigate the risks associated with the absence of address validation in the pair address argument, it is recommended to implement comprehensive address validation mechanisms. A recommended approach could be to verify pair existence in the decentralized application.

Prior to interacting with the pair address contract, perform checks to verify the existence and validity of the contract at the provided address. This can be achieved by querying the provider's contract or utilizing external libraries that provide contract verification services.

PLPI - Potential Liquidity Provision Inadequacy

Criticality	Minor / Informative
Location	DividendDistributor.sol#L636
Status	Unresolved

Description

The contract operates under the assumption that liquidity is consistently provided to the pair between the contract's token and the native currency. However, there is a possibility that liquidity is provided to a different pair. This inadequacy in liquidity provision in the main pair could expose the contract to risks. Specifically, during eligible transactions, where the contract attempts to swap tokens with the main pair, a failure may occur if liquidity has been added to a pair other than the primary one. Consequently, transactions triggering the swap functionality will result in a revert.

```
address[] memory path = new address[](2);
path[0] = address(_token);
path[1] = address(PAXG)
router.swapExactTokensForTokensSupportingFeeOnTransferTokens(
    amount,
    0,
    path,
    address(this),
    block.timestamp
```

Recommendation

The team is advised to implement a runtime mechanism to check if the pair has adequate liquidity provisions. This feature allows the contract to omit token swaps if the pair does not have adequate liquidity provisions, significantly minimizing the risk of potential failures.

Furthermore, the team could ensure the contract has the capability to switch its active pair in case liquidity is added to another pair.

Additionally, the contract could be designed to tolerate potential reverts from the swap functionality, especially when it is a part of the main transfer flow. This can be achieved by

executing the contract's token swaps in a non-reversible manner, thereby ensuring a more resilient and predictable operation.

PVC - Price Volatility Concern

Criticality	Minor / Informative
Location	DividendDistributor.sol#L897
Status	Unresolved

Description

The contract accumulates tokens from the taxes to swap them for ETH. The variable `swapThreshold` sets a threshold where the contract will trigger the swap functionality. If the variable is set to a big number, then the contract will swap a huge amount of tokens for ETH.

It is important to note that the price of the token representing it, can be highly volatile. This means that the value of a price volatility swap involving Ether could fluctuate significantly at the triggered point, potentially leading to significant price volatility for the parties involved.

```
    function swapBack() public swapping onlyToken {
        uint256 swapAmount =
swapThreshold.mul(marketingFee).div(totalBuyFee);
```

Recommendation

The contract could ensure that it will not sell more than a reasonable amount of tokens in a single transaction. A suggested implementation could check that the maximum amount should be less than a fixed percentage of the exchange reserves. Hence, the contract will guarantee that it cannot accumulate a huge amount of tokens in order to sell them.

RFV - Redundant Fee Variable

Criticality	Minor / Informative
Location	DividendDistributor.sol#L922,942
Status	Unresolved

Description

The contract is utilizing two separate variables, `sdgReceiverFee` and `buybackFee`, to calculate the total amount to be transferred to the `sdgFeeReceiver`. These variables are used to determine portions of the `swapThreshold` that correspond to different fees before being summed up for the final transfer amount. The calculation involves multiplying the `swapThreshold` by each fee and dividing by the `totalBuyFee`, resulting in `amountSDGReceiver` and `amountSDGBuyback` respectively. Subsequently, these amounts are added together for the transfer to sdgFeeReceiver. This approach, while mathematically sound, introduces unnecessary complexity and redundancy since the addition of these variables does not implement any additional functionality or differentiation in the handling of fees. Essentially, the contract is performing an extra step without a clear benefit, which could lead to confusion, increased gas costs, and potential errors in future modifications.

```
uint256 amountSDGReceiver = swapThreshold.mul(sdgReceiverFee).div(
    totalBuyFee
);
uint256 amountSDGBuyback = swapThreshold.mul(buybackFee).div(
    totalBuyFee
);
...
if (amountSDGReceiver > 0 || amountSDGBuyback > 0) {
    try
        IERC20(address(_token)).transfer(
            sdgFeeReceiver,
            amountSDGReceiver + amountSDGBuyback
        )
    {
        emit ReceiverAmount(amountSDGBuyback, amountSDGReceiver);
```

Recommendation

It is recommended to simplify the fee structure by consolidating `sdgReceiverFee` and `buybackFee` into a single variable. This can be achieved by either combining their values into a single fee variable or by re-evaluating the necessity of distinguishing these fees if they ultimately serve a similar purpose and are directed to the same receiver. Simplification will not only reduce the contract's complexity but also minimize potential points of failure and optimize gas costs associated with these calculations and transactions. Additionally, this change would make the contract more straightforward, enhancing its readability and maintainability. Future updates or audits will benefit from a clearer understanding of the fee handling mechanism, thereby reducing the risk of errors or unintended consequences.

RRS - Redundant Require Statement

Criticality	Minor / Informative
Location	ShadowGold.sol#L64 DividendDistributor.sol#L64
Status	Unresolved

Description

The contract utilizes a `require` statement within the `add` function aiming to prevent overflow errors. This function is designed based on the SafeMath library's principles. In Solidity version 0.8.0 and later, arithmetic operations revert on overflow and underflow, making the overflow check within the function redundant. This redundancy could lead to extra gas costs and increased complexity without providing additional security.

```
function add(uint256 a, uint256 b) internal pure returns (uint256) {
      uint256 c = a + b;
      require(c >= a, "SafeMath: addition overflow");
      return c;
}
```

Recommendation

It is recommended to remove the `require` statement from the add function since the contract is using a Solidity pragma version equal to or greater than 0.8.0. By doing so, the contract will leverage the built-in overflow and underflow checks provided by the Solidity language itself, simplifying the code and reducing gas consumption. This change will uphold the contract's integrity in handling arithmetic operations while optimizing for efficiency and cost-effectiveness.

RSML - Redundant SafeMath Library

Criticality	Minor / Informative
Location	ShadowGold.sol DividendDistributor.sol
Status	Unresolved

Description

SafeMath is a popular Solidity library that provides a set of functions for performing common arithmetic operations in a way that is resistant to integer overflows and underflows.

Starting with Solidity versions that are greater than or equal to 0.8.0, the arithmetic operations revert to underflow and overflow. As a result, the native functionality of the Solidity operations replaces the SafeMath library. Hence, the usage of the SafeMath library adds complexity, overhead and increases gas consumption unnecessarily in cases where the explanatory error message is not used.

```
library SafeMath {...}
```

Recommendation

The team is advised to remove the SafeMath library in cases where the revert error message is not used. Since the version of the contract is greater than `0.8.0` then the pure Solidity arithmetic operations produce the same result.

If the previous functionality is required, then the contract could exploit the `unchecked { ... }` statement.

Read more about the breaking change on https://docs.soliditylang.org/en/v0.8.16/080-breaking-changes.html#solidity-v0-8-0-breaking-changes.

OCTD - Transfers Contract's Tokens

Criticality	Minor / Informative
Location	ShadowGold.sol#L907 DividendDistributor.sol#L969
Status	Unresolved

Description

The contract owner has the authority to claim all the balance of the contract. The owner may take advantage of it by calling the `withdrawTokens` function.

```
   function withdrawTokens(address _token, uint256 _amount) public
onlyOwner {
        IERC20(_token).transfer(owner, _amount);
    }
...
    function withdrawTokens(address token, uint256 _amount) public
onlyOwner {
        IERC20(token).transfer(owner, _amount);
    }
```

Recommendation

The team should carefully manage the private keys of the owner's account. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the contract admin functions.

Temporary Solutions:

These measurements do not decrease the severity of the finding

- Introduce a time-locker mechanism with a reasonable delay.
- Introduce a multi-signature wallet so that many addresses will confirm the action.
- Introduce a governance model where users will vote about the actions.

Permanent Solution:

- Renouncing the ownership, which will eliminate the threats but it is non-reversible.

L04 - Conformance to Solidity Naming Conventions

Criticality	Minor / Informative
Location	ShadowGold.sol#L478,479,480,482,483,484,487,488,785,786,830,831,867,878,884,894,895,907,911,936,946,953,954 DividendDistributor.sol#L454,480,551,552,564,565,566,567,568,569,570,588,589,597,598,606,607,969
Status	Unresolved

Description

The Solidity style guide is a set of guidelines for writing clean and consistent Solidity code. Adhering to a style guide can help improve the readability and maintainability of the Solidity code, making it easier for others to understand and work with.

The followings are a few key points from the Solidity style guide:

1. Use camelCase for function and variable names, with the first letter in lowercase (e.g., myVariable, updateCounter).
2. Use PascalCase for contract, struct, and enum names, with the first letter in uppercase (e.g., MyContract, UserStruct, ErrorEnum).
3. Use uppercase for constant variables and enums (e.g., MAX_VALUE, ERROR_CODE).
4. Use indentation to improve readability and structure.
5. Use spaces between operators and after commas.
6. Use comments to explain the purpose and behavior of the code.
7. Keep lines short (around 120 characters) to improve readability.

```
string constant _name = "Test SDG"
string constant _symbol = "TSDG"
uint8 constant _decimals = 9
uint256 constant _totalSupply = 10 ** 8 * (10 ** _decimals)
uint256 constant _maxSupply = 10 ** 8 * (10 ** _decimals)
uint256 public _maxTxAmount
mapping(address => uint256) _balances
mapping(address => mapping(address => uint256)) _allowances
address _distributorContract
address _feeReceiver
uint256 _minPeriod
uint256 _minDistribution
uint256 GWEI
uint256 _amount

...
```

Recommendation

By following the Solidity naming convention guidelines, the codebase increased the readability, maintainability, and makes it easier to work with.
Find more information on the Solidity documentation
https://docs.soliditylang.org/en/v0.8.17/style-guide.html#naming-convention.

L06 - Missing Events Access Control

Criticality	Minor / Informative
Location	DividendDistributor.sol#L554
Status	Unresolved

Description

Events are a way to record and log information about changes or actions that occur within a contract. They are often used to notify external parties or clients about events that have occurred within the contract, such as the transfer of tokens or the completion of a task. There are functions that have no event emitted, so it is difficult to track off-chain changes.

```
_token = token
```

Recommendation

To avoid this issue, it's important to carefully design and implement the events in a contract, and to ensure that all required events are included. It's also a good idea to test the contract to ensure that all events are being properly triggered and logged.

By including all required events in the contract and thoroughly testing the contract's functionality, the contract ensures that it performs as intended and does not have any missing events that could cause issues.

L07 - Missing Events Arithmetic

Criticality	Minor / Informative
Location	ShadowGold.sol#L749,856,916,942,949
Status	Unresolved

Description

Events are a way to record and log information about changes or actions that occur within a contract. They are often used to notify external parties or clients about events that have occurred within the contract, such as the transfer of tokens or the completion of a task.

It's important to carefully design and implement the events in a contract, and to ensure that all required events are included. It's also a good idea to test the contract to ensure that all events are being properly triggered and logged.

```
totalShares = totalShares.sub(shares[shareholder].amount).add(amount)
launchedAt = launched_
transferBlockTime += _addSeconds
blackList[user] = flag;
authorizedContract[_authorizedContract] = flag;
```

Recommendation

By including all required events in the contract and thoroughly testing the contract's functionality, the contract ensures that it performs as intended and does not have any missing events that could cause issues with its arithmetic.

L11 - Unnecessary Boolean equality

Criticality	Minor / Informative
Location	ShadowGold.sol#L885 DividendDistributor.sol#L872
Status	Unresolved

Description

Boolean equality is unnecessary when comparing two boolean values. This is because a boolean value is either true or false, and there is no need to compare two values that are already known to be either true or false.

it's important to be aware of the types of variables and expressions that are being used in the contract's code, as this can affect the contract's behavior and performance. The comparison to boolean constants is redundant. Boolean constants can be used directly and do not need to be compared to true or false.

```
airdropped[_user] == false
wethOrPaxg == true
```

Recommendation

Using the boolean value itself is clearer and more concise, and it is generally considered good practice to avoid unnecessary boolean equalities in Solidity code.

L14 - Uninitialized Variables in Local Scope

Criticality	Minor / Informative
Location	ShadowGold.sol#L196,276,306,347 DividendDistributor.sol#L221,301,331,372,834,858,953
Status	Unresolved

Description

Using an uninitialized local variable can lead to unpredictable behavior and potentially cause errors in the contract. It's important to always initialize local variables with appropriate values before using them.

```
uint256 i
string memory reason
string memory e
```

Recommendation

By initializing local variables before using them, the contract ensures that the functions behave as expected and avoid potential issues.

L16 - Validate Variable Setters

Criticality	Minor / Informative
Location	DividendDistributor.sol#L554,559,560,591,592
Status	Unresolved

Description

The contract performs operations on variables that have been configured on user-supplied input. These variables are missing of proper check for the case where a value is zero. This can lead to problems when the contract is executed, as certain actions may not be properly handled when the value is zero.

```
_token = token
wethPair = _wethPair
paxgPair = _paxgPair
sdgFeeReceiver = _sdgFeeReceiver
marketingFeeReceiver = _marketingFeeReceiver
```

Recommendation

By adding the proper check, the contract will not allow the variables to be configured with zero value. This will ensure that the contract can handle all possible input values and avoid unexpected behavior or errors. Hence, it can help to prevent the contract from being exploited or operating unexpectedly.

L19 - Stable Compiler Version

Criticality	Minor / Informative
Location	ShadowGold.sol#L56 DividendDistributor.sol#L56
Status	Unresolved

Description

The `^` symbol indicates that any version of Solidity that is compatible with the specified version (i.e., any version that is a higher minor or patch version) can be used to compile the contract. The version lock is a mechanism that allows the author to specify a minimum version of the Solidity compiler that must be used to compile the contract code. This is useful because it ensures that the contract will be compiled using a version of the compiler that is known to be compatible with the code.

```
pragma solidity ^0.8.4;
```

Recommendation

The team is advised to lock the pragma to ensure the stability of the codebase. The locked pragma version ensures that the contract will not be deployed with an unexpected version. An unexpected version may produce vulnerabilities and undiscovered bugs. The compiler should be configured to the lowest version that provides all the required functionality for the codebase. As a result, the project will be compiled in a well-tested LTS (Long Term Support) environment.

L20 - Succeeded Transfer Check

Criticality	Minor / Informative
Location	ShadowGold.sol#L908 DividendDistributor.sol#L706,874,885,930,940,970
Status	Unresolved

Description

According to the ERC20 specification, the transfer methods should be checked if the result is successful. Otherwise, the contract may wrongly assume that the transfer has been established.

```
IERC20(_token).transfer(owner, _amount)
PAXG.transfer(shareholder, amount)
IERC20(WETH).transferFrom(msg.sender, address(this), amount)
IERC20(PAXG).transferFrom(msg.sender, address(this), amount)

IERC20(WETH).transfer(
                    marketingFeeReceiver,
                    amountWETHMarketing
                )

...
```

Recommendation

The contract should check if the result of the transfer methods is successful. The team is advised to check the SafeERC20 library from the Openzeppelin library.

Functions Analysis

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
ShadowAuth	Implementation			
		Public	✓	-
	authorizeFor	Public	✓	authorizedFor
	authorizeForMultiplePermissions	Public	✓	authorizedFor
	unauthorizeFor	Public	✓	authorizedFor
	unauthorizeForMultiplePermissions	Public	✓	authorizedFor
	isOwner	Public		-
	isAuthorizedFor	Public		-
	isAuthorizedFor	Public		-
	transferOwnership	Public	✓	onlyOwner
	getPermissionNameToIndex	Public		-
	getPermissionUnlockTime	Public		-
	isLocked	Public		-
	lockPermission	Public	✓	authorizedFor
	unlockPermission	Public	✓	-
TestSDG	Implementation	IERC20, ShadowAuth		
		Public	✓	ShadowAuth
		External	Payable	-

	totalSupply	External		-
	decimals	External		-
	symbol	External		-
	name	External		-
	getOwner	External		-
	balanceOf	Public		-
	allowance	External		-
	approve	Public	✓	-
	approveMax	External	✓	-
	transfer	External	✓	-
	transferFrom	External	✓	-
	_transferFrom	Internal	✓	
	_basicTransfer	Internal	✓	
	checkTxLimit	Internal		
	processFee	External	✓	-
	checkLaunched	External		-
	launched	Internal		
	launch	Internal	✓	
	setShare	External	✓	-
	getShare	External		-
	getTotalShares	External		-
	getTotalHolderCount	External		-
	getShareHolders	External		-

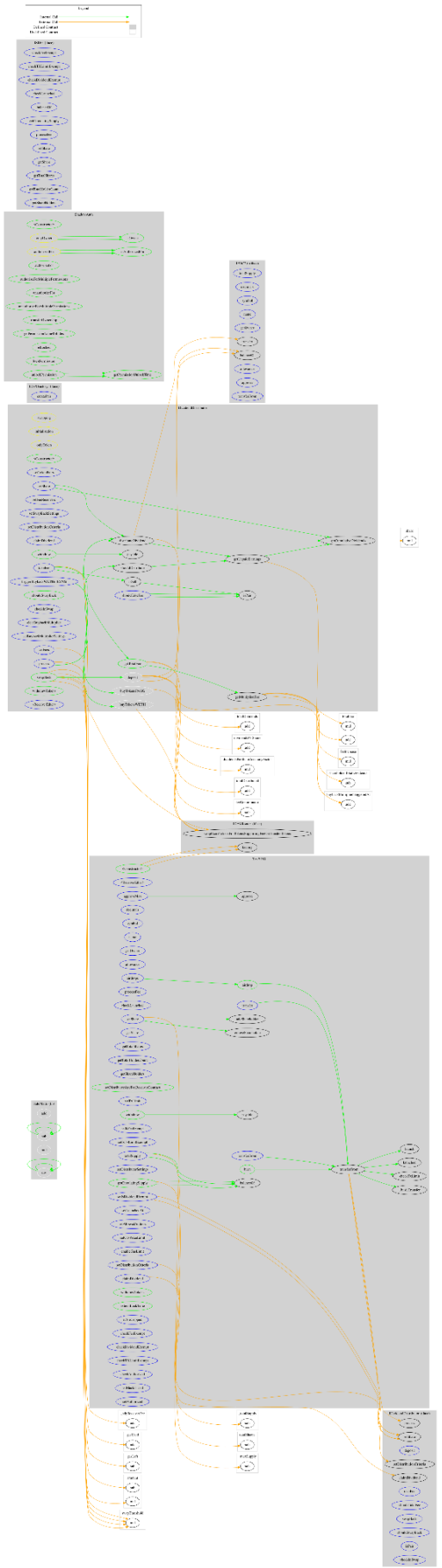
	addShareholder	Internal	✓	
	removeShareholder	Internal	✓	
	setDistributorAndFeeReceiverContract	Public	✓	onlyOwner
	setTxLimit	External	✓	authorizedFor
	setIsDividendExempt	External	✓	-
	setIsFeeExempt	External	✓	-
	setIsTxLimitExempt	External	✓	-
	setDistributionCriteria	External	✓	authorizedFor
	setDistributorSettings	External	✓	authorizedFor
	getCirculatingSupply	Public		-
	claimDividend	External	✓	-
	setLaunchedAt	External	✓	authorizedFor
	setAllowedAddress	External	✓	onlyOwner
	setGasPriceLimit	External	✓	onlyOwner
	enableGasLimit	External	✓	onlyOwner
	burn	Public	✓	-
	airdrop	Public	✓	onlyOwner
	airdrops	External	✓	onlyOwner
	withdraw	Public	✓	onlyOwner
	withdrawTokens	Public	✓	onlyOwner
	extendLockTime	Public	✓	onlyOwner
	isAirdropped	External		-
	checkFeeExempt	External		-

	checkDividendExempt	External		-
	checkTXLimitExempt	External		-
	checkAuthorized	External		-
	setBlackListed	External	✓	onlyOwner
	setAuthorized	External	✓	onlyOwner
DividendDistributor	Implementation	ShadowAuth		
		Public	✓	-
	setTokenPairs	External	✓	onlyOwner
	setFees	External	✓	authorizedFor
	setFeeReceivers	External	✓	authorizedFor
	setSwapBackSettings	External	✓	authorizedFor
	setDistributionCriteria	External	✓	onlyToken
	setShare	External	✓	onlyToken
	deposit	Internal	✓	
	process	External	✓	onlyToken
	shouldDistribute	Internal		
	distributeDividend	Internal	✓	
	claimDividend	External	✓	-
	isPair	Public		-
	shouldTakeFee	External		-
	getTotalFee	Public		-
	getMultipliedFee	Public		-

	takeFee	External	✓	onlyToken
	isSell	Internal		
	shouldSwapBack	Public		-
	checkInSwap	External		-
	clearBuybackMultiplier	External	✓	authorizedFor
	setBuybackMultiplierSettings	External	✓	authorizedFor
	buyTokensWETH	Internal	✓	swapping
	buyTokensPAXG	Internal	✓	swapping
	triggerBuybackWETHorPAXG	External	✓	authorizedFor
	swapBack	Public	✓	swapping onlyToken
	withdraw	Public	✓	onlyOwner
	withdrawTokens	Public	✓	onlyOwner
	getUnpaidEarnings	Public		-
	getCumulativeDividends	Internal		
		External	Payable	-

Inheritance Graph

Flow Graph



Summary

ShadowFi contract implements a token mechanism. This audit investigates security issues, business logic concerns and potential improvements. There are some functions that can be abused by the owner like stop transactions, manipulate the fees and blacklist addresses. A multi-wallet signing pattern will provide security against potential hacks. Temporarily locking the contract or renouncing ownership will eliminate all the contract threats.

Disclaimer

The information provided in this report does not constitute investment, financial or trading advice and you should not treat any of the document's content as such. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes nor may copies be delivered to any other person other than the Company without Cyberscope's prior written consent. This report is not nor should be considered an "endorsement" or "disapproval" of any particular project or team. This report is not nor should be regarded as an indication of the economics or value of any "product" or "asset" created by any team or project that contracts Cyberscope to perform a security assessment. This document does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors' business, business model or legal compliance. This report should not be used in any way to make decisions around investment or involvement with any particular project. This report represents an extensive assessment process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk Cyberscope's position is that each company and individual are responsible for their own due diligence and continuous security Cyberscope's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies and in no way claims any guarantee of security or functionality of the technology we agree to analyze. The assessment services provided by Cyberscope are subject to dependencies and are under continuing development. You agree that your access and/or use including but not limited to any services reports and materials will be at your sole risk on an as-is where-is and as-available basis Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives false negatives and other unpredictable results. The services may access and depend upon multiple layers of third parties.

About Cyberscope

Cyberscope is a blockchain cybersecurity company that was founded with the vision to make web3.0 a safer place for investors and developers. Since its launch, it has worked with thousands of projects and is estimated to have secured tens of millions of investors' funds.

Cyberscope is one of the leading smart contract audit firms in the crypto space and has built a high-profile network of clients and partners.

The Cyberscope team

https://www.cyberscope.io