Security Assessment

DUST SWAP

Verified On Feb 4th, 2024

@Vital-Block

@VB_Audit

info@vitalblock.org

www.vitalblock.org

PREPARED FOR:

DUST SWAP

TABLE OF CONTENTS

Document Properties

Client	Dust Swap
Title	Smart Contract Audit Report
Target	DUST SWAP
Audit Version	1.0
Author	Akhmetshin Marat
Auditors	Akhmetshin Marat, James BK, Benny Matin
Reviewed by	Dima Meru
Approved by	Prince Mitchell
Classification	Public

Version Info

Version	Date	Author(s)	Description
1.0	February 04, 2024	James BK	Final Released
1.0-AP	January 04, 2024	Benny Matin	Release Candidate

Contact

For more information about this document and its contents, please contact Vital Block Security Inc.

Name	Akhmetshin Marat
Phone	+44 7944 248057
Email	info@vitalblock.org

In the following, we show the specific pull request and the commit hash value used in this audit.

- https://github.com/DustSwapOfficial/contract (AX2P590)
- https://github.com/DustSwapOfficial/contract/tree/main/token (9dYf778)

About Vital Block Security

Vital Block Security provides professional, thorough, fast, and easy-to-understand smart contract security audit. We do in-depth and penetrative static, manual, automated, and intelligent analysis of the smart contract. Some of our automated scans include tools like ConsenSys MythX, Mythril, Slither, Surya. We can audit custom smart contracts, DApps, Rust, NFTs, etc (including the service of smart contract auditing). We are reachable at Telegram (https://t.me/vital_block), Twitter (http://twitter.com/Vb_Audit), or Email (info@vitalblock.org).

Table 1.2: Vulnerability Severity Classification

Impact \ Likelihood	*High*	*Medium*	*Low*
High	Critical	High	Medium
Medium	High	Medium	Low
Low	Medium	Low	Low

Methodology (1)

To standardize the evaluation, we define the following terminology based on the OWASP Risk Rating Methodology [4]:

- Likelihood represents how likely a particular vulnerability is to be uncovered and exploited in the wild;
- Impact measures the technical loss and business damage of a successful attack;
- Severity demonstrates the overall criticality of the risk.

SCOPE OF WORK

Vital Block was consulted by DUST SWAP to conduct the smart contract audit of its Rust source code. The audit scope of work is strictly limited to mentioned .Rust file only:

`Odustswap`**.sol**

ℹ️ **External contracts and/or interfaces dependencies are not checked due to being out of scope.**

Verify audited contract code Repo.

Public Contract Link
https://github.com/DustSwapOfficial/contract/tree/main/token
https://github.com/DustSwapOfficial/contract/tree/main/router
https://github.com/DustSwapOfficial/contract/tree/main/router/contracts
https://github.com/DustSwapOfficial/contract/tree/main/factory
https://github.com/DustSwapOfficial/contract/tree/main/factory/contracts
https://github.com/DustSwapOfficial/contract/blob/main/token/DustToken.sol

AUDIT METHODOLOGY

Smart contract audits are conducted using a set of standards and procedures. Mutual collaboration is essential to performing an effective smart contract audit. Here's a brief overview of Vital Block Security auditing process and methodology:

CONNECT

- The onboarding team gathers source codes, and specifications to make sure we understand the size, and scope of the smart contract audit.

AUDIT

- Automated analysis is performed to identify common contract vulnerabilities. We may use the following third-party frameworks and dependencies to perform the automated analysis:
  - Remix IDE Developer Tool
  - Open Zeppelin Code Analyzer
  - SWC Vulnerabilities Registry
  - DEX Dependencies, e.g., Pancakeswap, Uniswap
- Simulations are performed to identify centralized exploits causing contract and/or trade locks.
- A manual line-by-line analysis is performed to identify contract issues and centralized privileges. We may inspect below mentioned common contract vulnerabilities, and centralized exploits:

Centralized Exploits	○ Token Supply Manipulation ○ Access Control and Authorization ○ Assets Manipulation ○ Ownership Control ○ Liquidity Access ○ Stop and Pause Trading ○ Ownable Library Verification

Common Contract Vulnerabilities	○ Integer Overflow ○ Lack of Arbitrary limits ○ Incorrect Inheritance Order ○ Typographical Errors ○ Requirement Violation ○ Gas Optimization ○ Coding Style Violations ○ Re-entrancy ○ Third-Party Dependencies ○ Potential Sandwich Attacks ○ Irrelevant Codes ○ Divide before multiply ○ Conformance to Solidity Naming Guides ○ Compiler Specific Warnings ○ Language Specific Warnings

REPORT

- The auditing team provides a preliminary report specifying all the checks which have been performed and the findings thereof.
- The client's development team reviews the report and makes amendments to the codes.
- The auditing team provides the final comprehensive report with open and unresolved issues.

PUBLISH

- The client may use the audit report internally or disclose it publicly.

ℹ️ It is important to note that there is no pass or fail in the audit, it is recommended to view the audit as an unbiased assessment of the safety of solidity codes.

Table 1.0 The Full Audit Checklist

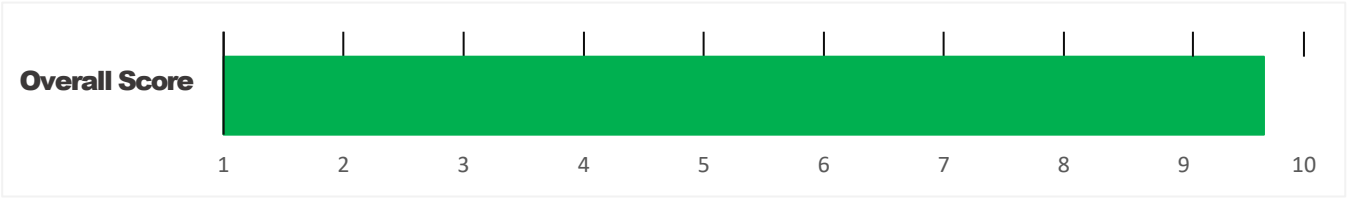
Category	Checklist Items
Basic Coding Bugs	Constructor Mismatch
	Ownership Takeover
	Redundant Fallback Function
	Overflows & Underflows
	Reentrancy
	Money-Giving Bug
	Blackhole
	Unauthorized Self-Destruct
	Revert DoS
	Unchecked External Call
	Gasless Send
	Send Instead Of Transfer
	Costly Loop
	(Unsafe) Use Of Untrusted Libraries
	(Unsafe) Use Of Predictable Variables
	Transaction Ordering Dependence
	Deprecated Uses
Semantic Consistency Checks	Semantic Consistency Checks
Advanced DeFi Scrutiny	Business Logics Review
	Functionality Checks
	Authentication Management
	Access Control & Authorization
	Oracle Security
	Digital Asset Escrow
	Kill-Switch Mechanism
	Operation Trails & Event Generation
	ERC20 Idiosyncrasies Handling
	Frontend-Contract Integration
	Deployment Consistency
	Holistic Risk Management
Additional Recommendations	Avoiding Use of Variadic Byte Array
	Using Fixed Compiler Version
	Making Visibility Level Explicit
	Making Type Inference Explicit
	Adhering To Function Declaration Strictly
	Following Other Best Practices

EXECUTIVE SUMMARY

Vital Block Security has performed the automated and manual analysis of the DUST SWAP Sol code. The code was reviewed for common contract vulnerabilities and centralized exploits. Here's a quick audit summary:

Status	Critical !	Major "	Medium #	Minor $	Unknown %
Open	0	0	0	1	0
Acknowledged	0	0	1	3	0
Resolved	0	0	1	0	2
Noteworty onlyOwner Privileges	Set Taxes and Ratios, Airdrop, Set Protection Settings, Set Reward Properties, Set Reflector Settings, Set Swap Settings, Set Pair and Router				

DUST SWAP Smart contract has achieved the following score: 97.0



Please note that smart contracts deployed on blockchains aren't resistant to exploits, vulnerabilities and/or hacks. Blockchain and cryptography assets utilize new and emerging technologies. These technologies present a high level of ongoing risks. For a detailed understanding of risk severity, source code vulnerability, and audit limitations, kindly review the audit report thoroughly.

Please note that centralization privileges regardless of their inherited risk status - constitute an elevated impact on smart contract safety and security.

CENTRALIZED PRIVILEGES

Centralization risk is the most common cause of cryptography asset loss. When a smart contract has a privileged role, the risk related to centralization is elevated.

There are some well-intended reasons have privileged roles, such as:

- **Privileged roles can be granted the power to** pause() **the contract in case of an external attack.**
- **Privileged roles can use functions like,** include(), **and** exclude() **to add or remove wallets from fees, swap checks, and transaction limits. This is useful to run a presale and to list on an exchange.**

Authorizing privileged roles to externally-owned-account (EOA) is dangerous. Lately, centralization-related losses are increasing in frequency and magnitude.

- **The client can lower centralization-related risks by implementing below mentioned practices:**
- **Privileged role's private key must be carefully secured to avoid any potential hack.**
- **Privileged role should be shared by multi-signature (multi-sig) wallets.**
- **Authorized privilege can be locked in a contract, user voting, or community DAO can be introduced to unlock the privilege.**
- **Renouncing the contract ownership, and privileged roles.**
- **Remove functions with elevated centralization risk.**

ℹ️ **Understand the project's initial asset distribution. Assets in the liquidity pair should be locked. Assets outside the liquidity pair should be locked with a release schedule.**

RISK CATEGORIES

Smart contracts are generally designed to hold, approve, and transfer tokens. This makes them very tempting attack targets. A successful external attack may allow the external attacker to directly exploit. A successful centralization-related exploit may allow the privileged role to directly exploit. All risks which are identified in the audit report are categorized here for the reader to review:

Risk Type	Definition
Critical !	These risks could be exploited easily and can lead to asset loss, data loss, asset, or data manipulation. They should be fixed right away.
Major "	These risks are hard to exploit but very important to fix, they carry an elevated risk of smart contract manipulation, which can lead to high-risk severity.
Medium #	These risks should be fixed, as they carry an inherent risk of future exploits, and hacks which may or may not impact the smart contract execution. Low-risk re-entrancy-related vulnerabilities should be fixed to deter exploits.
Minor $	These risks do not pose a considerable risk to the contract or those who interact with it. They are code-style violations and deviations from standard practices. They should be highlighted and fixed nonetheless.
Unknown %	These risks pose uncertain severity to the contract or those who interact with it. They should be fixed immediately to mitigate the risk uncertainty.

All statuses which are identified in the audit report are categorized here for the reader to review:

Status Type	Definition
Open	Risks are open.
Acknowledged	Risks are acknowledged, but not fixed.
Resolved	Risks are acknowledged and fixed.

Key Findings

Overall, these contracts are well-designed and engineered, though the implementation can be improved by resolving the identified issues (shown in Table 2.1), 2 medium-severity vulnerabilities, 3 low-severity vulnerabilities, and 2 informational recommen- dations.

Table 2.1: Key Lenny Token Audit Findings

ID	Severity	Title	Category	Status
LNY-001	Informational	In updateForMinter , the following equation is used inside an unchecked block	Coding Practice	Fixed
LNY-002	Low	In updateFormapping , the following equation is used inside an unchecked block	Business Logic	Fixed
LNY-003	Low	In updateForAmount, Relevant Function Snippet	Coding Practice	Fixed
LNY-004	Informational	updateForbalance, Relevant Function Snippet	Coding Practice	Fixed
LNY-005	Acknowledge	In updateForOwner, Relevant Function Snippet	Business Logic	Fixed

Beside the identified issues, we emphasize that for any user-facing applications and services, it is always important to develop necessary risk-control mechanisms and make contingency plans, which may need to be exercised before the mainnet deployment. The risk-control mechanisms should kick in at the very moment when the contracts are being deployed on mainnet. Please refer to page 10 for details.

AUDIT SCOPE | DUST SWAP

ID	Repo	Comment	File	SHM321 Checksum
DBY	DustSwapOfficial/contract/tree/main/token	cC512486	DustToken.sol	6788099YIRHVSK853PKFMGHEF44309200KDHFCBUGIJN
DBI	DustSwapOfficial/contract/tree/main/token	cC512486	DustToken.sol	347520JHDB7549H22H3BVDIOETYUHF009JBIKBDI33BJ4
DBW	DustSwapOfficial/contract/tree/main/token	cC512486	DustToken.sol	1988Y73HUGFDINN353840NFMTEJER73649RGFIMDIDH
DBG	DustSwapOfficial/contract/tree/main/token	cC512486	DustToken.sol	4438648TEOHBF6378309EHROECNEPOEJDNETE8EYEU3
DBL	DustSwapOfficial/contract/tree/main/token	cC512486	DustToken.sol	66390028765RVNKDBYFTGW553T2KOEHIUUJJIJE
DBA	DustSwapOfficial/contract/tree/main/token	cC512486	DustToken.sol	09825539BDYG543DVNKOMIKEBYRJUFHHFHJFIE333222
DBJ	DustSwapOfficial/contract/tree/main/router	cC512486	DustSwapRouter.sol	8654RJVT3DWI865YK26437903JJDGGDHGWY6E
DBE	DustSwapOfficial/contract/tree/main/router	cC512486	DustSwapRouter.sol	7763888636TGYGFFTFHBETT66TFTCTVYBHBYT
DBP	DustSwapOfficial/contract/tree/main/router	cC512486	DustSwapRouter.sol	88530486494YRHFTEICBGEIEGWTWYWUHEJEHEIE33U3
DBM	DustSwapOfficial/contract/tree/main/router	cC512486	DustSwapRouter.sol	1209873KHJLKJNFJHGE98763990029774BCUHHDUU239
DBV	DustSwapOfficial/contract/tree/main/factory	cC512486	DustswapFactory.sol	23456UGFYUHE98756EFHJHE7654ESDFGHGERTYUJ3897
DBQ	DustSwapOfficial/contract/tree/main/factory	cC512486	DustswapFactory.sol	37889UHBIONEO7TYRDFGVBN5678939IJWSFVDYUHDCI
DBS	DustSwapOfficial/contract/tree/main/factory	cC512486	DustswapFactory.sol	678903098TFHJKFCPOIUGFGHJKE9865ERGBEIVBHE8767
DBR	DustSwapOfficial/contract/tree/main/factory	cC512480	DustswapFactory.sol	98765SDFGBNFCOI56789UIYHGGHEJDIUYTRDCVBN3459
DCD	contract/tree/main/factory/contracts	cC512481	DustswapFactory.sol	3348y9808hgtrusvnmu43100ejfojgfnut8496230hb574he
DHU	contract/tree/main/factory/contracts	cC512481	DustswapFactory.sol	9864byf5f379eig28ffre64085jv1613251guhkdmue87
DGG	contract/tree/main/factory/contracts	cC512481	DustswapFactory.sol	7ej2d8jg765tjfiowg538ij74dwftyv6478ij3gs820
DTR	contract/tree/main/factory/contracts	cC512481	DustswapFactory.sol	864fr46de438hdguw903rfdcb246dbuhb2917enk

AUTOMATED ANALYSIS

Symbol	Definition
	**Function modifies state**
	**Function is payable**
	**Function is internal**
	**Function is private**
	Function is important

DUST SWAP	Interface			
└	totalSupply	External !		! |NO!
└	decimals	External !		! |NO!
└	symbol	External !		! |NO!
└	name	External !		! |NO!
└	getOwner	External !		|NO!
└	balanceOf	External !		! |NO!
└	transfer	External !	"	! |NO!
└	allowance	External !		! |NO!
└	approve	External !	"	! |NO!
└	transferFrom	External !	"	|NO!

IFactoryV2	Interface		
└	getPair	External !	|NO!
└	createPair	External !	" |NO!

IV2Pair	Interface		
└	factory	External !	|NO!
└	getReserves	External !	|NO!
└	sync	External !	" |NO!

IRouter01	Interface			
└	factory	External ❗		|NO❗
└	ETH	External ❗		|NO❗
└	addLiquidityETH	External ❗		# |NO❗
└	addLiquidity	External ❗	"	|NO❗
└	swapExactETHForTokens	External ❗		# |NO❗
└	getAmountsOut	External ❗		|NO❗
└	getAmountsIn	External ❗		|NO❗
IRouter02	Interface	IRouter01		
└	swapExactTokensForETHSupportingFeeOnTransferTokens	External ❗	"	|NO❗
└	swapExactETHForTokensSupportingFeeOnTransferTokens	External ❗		# |NO❗
└	swapExactTokensForTokensSupportingFeeOnTransferTokens	External ❗	" ! 🛑 |NO❗
└	swapExactTokensForTokens	External ❗	"	|NO❗
Protections	Interface			
└	checkUser	External ❗	" ! 🛑 |NO❗
└	setLaunch	External ❗	" ! 🛑 |NO❗
└	setLpPair	External ❗	" ! 🛑 |NO❗
└	**DUST**	External ❗	" |NO❗
└	removeSniper	External ❗	" |NO❗
Cashier	Interface			
└	setRewardsProperties	External ❗	"	|NO❗
└	tally	External ❗	" |NO❗
└	load	External ❗		# |NO❗
└	cashout	External ❗	"	|NO❗
└	giveMeWelfarePlease	External ❗	"	|NO❗
└	getTotalDistributed	External ❗		|NO❗
└	getUserInfo	External ❗		|NO❗
└	getUserRealizedRewards	External ❗		|NO❗

└	getPendingRewards	External ❗		|NO❗
└	initialize	External ❗	"	|NO❗
└	getCurrentReward	External ❗		|NO❗
SOL	Implementation	SafeMath		
└	<Constructor>	Public ❗		# |NO❗
└	transferOwner	External ❗	"		onlyOwner
└	renounceOwnership	External ❗	"		NO❗
└	setOperator	Public ❗	"	|NO❗
└	renounceOriginalDeployer	External ❗	"	|NO❗
└	<Receive Ether>	External ❗		# |NO❗
└	totalSupply	External ❗		|NO❗
└	decimals	External ❗		|NO❗
└	symbol	External ❗		|NO❗
└	name	External ❗		|NO❗
└	getOwner	External ❗		❗ |NO❗
└	balanceOf	Public ❗		❗ |NO❗
└	allowance	External ❗		❗ |NO❗
└	approve	External ❗	"	❗ 🛑 |NO❗
└	_approve	Internal $	"		
└	approveContractContingency	Public ❗	"	❗ 🛑	onlyOwner
└	transfer	External ❗	"	|NO❗
└	transferFrom	External ❗	"	|NO❗
└	setNewRouter	External ❗	"		onlyOwner
└	setLpPair	External ❗	"		onlyOwner
└	setInitializers	External ❗	"		onlyOwner
└	isExcludedFromFees	External ❗		|NO❗
└	isExcludedFromDividends	External ❗		|NO❗
└	isExcludedFromProtection	External ❗		|NO❗
└	setDividendExcluded	Public ❗	"		onlyOwner
└	setExcludedFromFees	Public ❗	"		onlyOwner

OPTIMIZATIONS | DUST SWAP

ID	Title	Category	Status
DTV	Logarithm Refinement Optimization	Gas Optimization	Acknowledged
DOP	Checks Can Be Performed Earlier	Gas Optimization	Acknowledged
DDP	Unnecessary Use Of SafeMath	Gas Optimization	Acknowledged
DWY	Struct Optimization	Gas Optimization	Acknowledged
DGT	Unused State Variable	Gas Optimization	Acknowledged

General Detectors

Public Functions Should be Declared External

Some functions in this contract should be declared as external in order to save gas

Attention Required

Missing Zero Address Validation

Some functions in this contract may not appropriately check for zero addresses being used.

Attention Required

Numeric Notation Best Practices

The numeric notation used in this contract is unconventional, possibly worsening the reading/debugging experience

Attention Required

- No compiler version inconsistencies found
- No unchecked call responses found
- No vulnerable self-destruct functions found
- No assertion vulnerabilities found
- No old solidity code found
- No external delegated calls found
- No external call dependency found
- No vulnerable authentication calls found
- No invalid character typos found
- No RTL characters found
- No dead code found
- No risky data allocation found
- No uninitialized state variables found
- No uninitialized storage variables found
- No vulnerable initialization functions found
- No risky data handling found
- No number accuracy bug found
- No out-of-range number vulnerability found
- No map data deletion vulnerabilities found
- No tautologies or contradictions found
- No faulty true/false values found
- No innacurate divisions found
- No redundant constructor calls found
- No vulnerable transfers found
- No vulnerable return values found
- No uninitialized local variables found
- No default function responses found
- No missing arithmetic events found
- No missing access control events found
- No redundant true/false comparisons found
- No state variables vulnerable through function calls found
- No buggy low-level calls found
- No expensive loops found
- No bad numeric notation practices found
- No missing constant declarations found
- No missing external function declarations found
- No vulnerable payable functions found
- No vulnerable message values found

Vulnerability Run check

Dust Swap / DUST
04/02/2024 06:15 AM UTC+8

Contract Info

Total supply	1000000000
Transaction Tax	Buy 0.00% / Sell 0.00%

Risk Analysis

Contract source code verified

This token contract is open source. You can check the contract code for details. Unsourced token contracts are likely to have malicious functions to defraud their users of their assets.

No Proxy

There is no proxy in the contract. The proxy contract means contract owner can modify the function of the token and possibly effect the price.

No mint function

Mint function is transparent or non-existent. Hidden mint functions may increase the amount of tokens in circulation and effect the price of the token.

No function to retrieve ownership

If this function exists, it is possible for the project owner to regain ownership even after relinquishing it.

Owner cant change balance

The contract owner does not have the authority to modify the balance of tokens at other addresses.

Honeypot Risk

This does not appear to be a honeypot

We are not aware of any code that prevents the sale of tokens.

No trading cooldown

The token contract has no trading cooldown function.If there is a trading cooldown function, the user will not be able to sell the token within a certain time or block after buying.

No Anti Whale

There is no limit to the number of token transactions. The number of scam token transactions may be limited (honeypot risk).

No blacklist function

No blacklist function is included.

No whitelist function

Whitelist function found

Holders

Holder count

0x62...c66b

Creator

OWNERSHIP NOT RENOUNCED

0x62...c66b

Owner

...

Liquidity Pool

DNY-01 Key Findings

Category	Severity ●	Location	Status
Status Mathematical Operations	Low	Multiple Contracts	Informational

Description

In **updateForMinter ,** the following equation is used inside an unchecked block

```
function _mint(address account, uint256 amount) internal virtual {
    require(account != address(0), "ERC20: mint to the zero address");

    _beforeTokenTransfer(address(0), account, amount);

    _totalSupply += amount;
    _balances[account] += amount;
    emit Transfer(address(0), account, amount);
}
```

Minter can not issue more **DUST SWAP** Token indefinitely.
Note that as of the date of publishing, the above review reflects the current understanding of known security patterns as they relate to the **DUST SWAP** contract.

Thus, this enables the approval of a token account for confidential transfers, even if it is associated with a different mint. Ideally, token accounts should only be allowed to hold tokens from the specific mint they are associated with. By not checking the mint consistency, the function effectively approves arbitrary token accounts for confidential transfers. Such unauthorized token mixing may have security and financial implications, as it could result in loss of value or assets for users who rely on the token system's integrity.

Recommendation

Incorporate the following verification within process approve account to confirm that the token account's associated mint aligns with the mint for which the confidential transfer approval is sought.

DNY-02 Key Findings

Category	Severity	Target	Status
Business Logic	Medium	token/DustToken.sol	Fixed

Description

In **updateFormapping ,** the following equation is used inside an unchecked block

```
contract Dust is Context, IERC20, IERC20Metadata {
    mapping(address => uint256) private _balances;

    mapping(address => mapping(address => uint256)) private _allowances;
```

Description

The function mapping () does not have the override specifier. It should be noted that since (> a function that overrides only a single interface function does not require the override specifier (see doc). However, all other instances of this in the code base contain the override specifier.

Recommendation

We recommend either checking for overflow in this case, or ensuring that the **PairsIn** is close enough it will never cause an overflow

LNY-03 Key Findings

Category	Severity	Target	Status
Inconsistency	Informational	Multiple Contracts	Acknowledge

Description

In **updateForAmount**, Relevant Function Snippet

```
function transfer(address recipient, uint256 amount)
        public
        virtual
        override
        returns (bool)
    {
        _transfer(_msgSender(), recipient, amount);
        return true;
    }
```

Description

The function amount0 () does not have the override specifier. It should be noted that since amount0 > a function That overrides only a single interface function does not require the override specifier. However, all other instances of this in the codebase contain the override specifier

Recommendation

We recommend adding the override specifier to amount() or removing the override specifier from all other functions this applies to for consistency.

DDL-04 Key Findings

Category	Severity	Target	Status
Coding Practices	low	factory/contracts/DustswapFactory.sol	Confirmed

Description

updateForbalance, Relevant Function Snippet

```
function _burn(address account, uint256 amount) internal virtual {
    require(account != address(0), "ERC20: burn from the zero address");

    _beforeTokenTransfer(account, address(0), amount);

    uint256 accountBalance = _balances[account];
    require(accountBalance >= amount, "ERC20: burn amount exceeds balance");
    _balances[account] = accountBalance - amount;
    _totalSupply -= amount;

    emit Transfer(account, address(0), amount);
}
```

Description

While re-viewing arithmetic operations in current balance implementation, we notice occasions that may introduce unexpected overflows/underflows.

For example, if we examine the `helpers::query_balance(&deps, &sender);` function, it may revert if the current `collateralData` is equal to `0`. Another example is when the underlying asset of a recipient has an unusual decimal, which may revert the following calculation of `if sender == &collect_tax_wallet || recipient == &collect_tax_wallet {`

```
assert_eq!(
```

Note this calculation appears in a num- ber of routines. Its revert may bring in unnecessary frictions and cause issues for integration and composability.

Recommendation

Revise the above calculation to avoid the unnecessary overflows and under- flows.

LNY-06 Key Findings

Category	Severity	Target	Status
Coding Practices	low	router/contracts/DustSwapRouter.sol	Informational

Description

In **updateForOwner**, Relevant Function Snippet

```
 */
function _approve(
    address owner,
    address spender,
    uint256 amount
) internal virtual {
    require(owner != address(0), "ERC20: approve from the zero address");
    require(spender != address(0), "ERC20: approve to the zero address");

    _allowances[owner][spender] = amount;
    emit Approval(owner, spender, amount);
}
```

Description

For Ownership efficiency, the Lenny Token is engineered with the reserve cache mechanism, which necessi-tates the common steps to be followed when operating with the reserve Ownership data in different scenarios, including the tax generation, update, and eventual persistence.

Recommendation

Revise the above functions to following a consistent approach to use the reserve cache mechanism.

Vulnerability Scan

REENTRANCY

No reentrancy risk found

Severity	Major
Confidence Parameter	Certain

Vulnerability Description

Mintable: More amount of the DUST SWAP token can **NOT** be minted by a private wallet or contract. **(This is Essentially normal for most contracts)**

Scanning Line:

```
function _mint(address account, uint256 amount) internal virtual {
        require(account != address(0), "ERC20: mint to the zero
address");

        _beforeTokenTransfer(address(0), account, amount);

        _totalSupply += amount;
        _balances[account] += amount;
        emit Transfer(address(0), account, amount);
    }
```

Repository:

https://github.com/DustSwapOfficial/contract

Audited Files

DustswapFactory.sol
DustSwapRouter.sol
DustToken.sol

Contract Creator Address

0x62CAFe1AD6A32bA04410356Eb399d4c1F947C66B

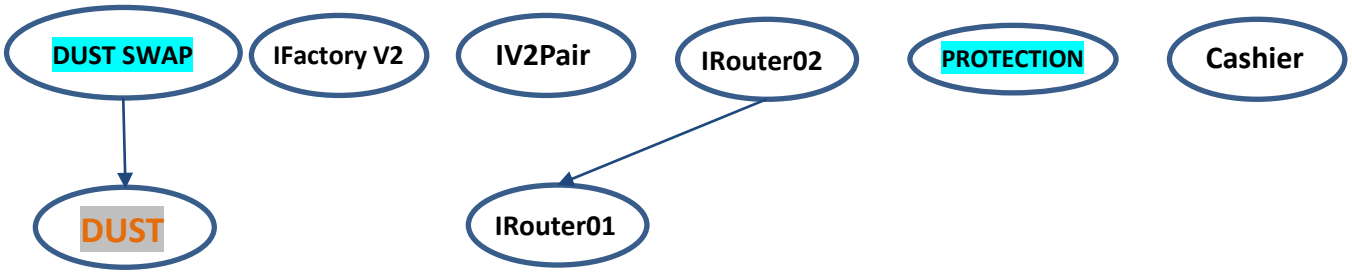
Deployed Contracts:

0x65F6045b66C47af52B94556f879Ca39A0C1F9aD3

Creator TXH Contracts:

https://etherscan.io/tx/0xbe386270703653fcfb15bbb930513925b6758bded3d5a59a560fbf003486bcd2

INHERITANCE GRAPH



Identifier	Definition	Severity
CEN-12	Centralization privileges of DUST SWAP	Medium #

Vulnerability 0 : No important security issue detected.
Threat level: Low

ISSUES CHECKING STATUS

	Issue Description	Checking Status
1.	Compiler errors.	PASSED
2.	Race Conditions and reentrancy. Cross-Function Race Conditions.	PASSED
3.	Possible Delay In Data Delivery.	PASSED
4.	Oracle calls.	PASSED
5.	Front Running.	PASSED
6.	Sol. Dependency.	PASSED
7.	Integer Overflow And Underflow.	PASSED
8.	DoS with Revert.	PASSED
9.	Dos With Block Gas Limit.	PASSED
10.	Methods execution permissions.	PASSED
11.	Economy Model of the contract.	PASSED
12.	The Impact Of Exchange Rate On the solidity Logic.	PASSED
13.	Private use data leaks.	PASSED
14.	Malicious Event log.	PASSED
15.	Scoping and Declarations.	PASSED
16.	Uninitialized storage pointers.	PASSED
17.	Arithmetic accuracy.	PASSED
18.	Design Logic.	PASSED
19.	Cross-Function race Conditions	PASSED
20.	Save Upon solidity contract Implementation and Usage.	PASSED
21.	Fallback Function Security	PASSED

AUDIT RESULT

PASSED

MANUAL REVIEW

Dust Swap functions as a smooth, streamlined decentralized exchange (DEX) within the Linea network. Thanks to the incorporation of zero-knowledge technology, Dust Swap paves the way for an effortless and affordable DeFi experience, backed by the robust security of Ethereum.

TOKEN NAME: DUST SWAP
Ticker: DUST
Total Supply: 1,000,000,000

The DUST SWAP Platform Is Launching On The LINEA Network

Identifier	Definition	Severity
CEN-02	Initial asset distribution	Minor

All of the initially minted assets are sent to the contract deployer when deploying the contract. This is Normal for most deployer and/or contract owner .

```
function decreaseAllowance(address spender, uint256 subtractedValue)
        public
        virtual
        returns (bool)
    {
        uint256 currentAllowance = _allowances[_msgSender()][spender];
        require(
            currentAllowance >= subtractedValue,
```

RECOMMENDATION

Project stakeholders should be consulted during the initial asset distribution process.

RECOMMENDATION

Deployer and/or contract owner private keys are secured carefully.

Please refer to PAGE-10 CENTRALIZED PRIVILEGES for a detailed understanding.

ALLEVIATION

The DUST SWAP project team understands the centralization risk. Some functions are provided privileged access to ensure a good runtime behavior in the project

References

1 MITRE. CWE-1041: Use of Redundant Code. https://cwe.mitre.org/data/definitions/1041.html.

2 MITRE. CWE-1099: Inconsistent Naming Conventions for Identifiers. https://cwe.mitre.org/data/definitions/1099.html.

3 MITRE. CWE-561: Dead Code. https://cwe.mitre.org/data/definitions/561.html.

4 MITRE. CWE-563: Assignment to Variable without Use. https://cwe.mitre.org/data/definitions/563.html.

5 MITRE. CWE-663: Use of a Non-reentrant Function in a Concurrent Context. https://cwe.mitre.org/data/definitions/663.html.

6 MITRE. CWE-837: Improper Enforcement of a Single, Unique Action. https://cwe.mitre.org/data/definitions/837.html.

7 MITRE. CWE-841: Improper Enforcement of Behavioral Workflow. https://cwe.mitre.org/data/definitions/841.html.

8 MITRE. CWE CATEGORY: Bad Coding Practices. https://cwe.mitre.org/data/definitions/1006.html.

9 MITRE. CWE CATEGORY: Business Logic Errors. https://cwe.mitre.org/data/definitions/840.html.

10 MITRE. CWE CATEGORY: Concurrency. https://cwe.mitre.org/data/definitions/557.html.

11 MITRE. CWE VIEW: Development Concepts. https://cwe.mitre.org/data/definitions/699.html.

12 OWASP. Risk Rating Methodology. https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology.

Identifier	Definition	Severity
COD-10	Third Party Dependencies	Minor

Smart contract is interacting with third party protocols e.g., Pancakeswap router, cashier contract, protections contract. The scope of the audit treats third party entities as black boxes and assumes their functional correctness. However, in the real world, third parties can be compromised, and exploited. Moreover, upgrades in third parties can create severe impacts, e.g., increased transactional fees, deprecation of previous routers, etc.

RECOMMENDATION

Inspect and validate third party dependencies regularly, and mitigate severe impacts whenever necessary.

DISCLAIMERS

Vital Block Security provides the easy-to-understand audit of Solidity, Move and Raw source codes (commonly known as smart contracts).

The smart contract for this particular audit was analyzed for common contract vulnerabilities, and centralization exploits. This audit report makes no statements or warranties on the security of the code. This audit report does not provide any warranty or guarantee regarding the absolute bug-free nature of the smart contract analyzed, nor do they provide any indication of the client's business, business model or legal compliance. This audit report does not extend to the compiler layer, any other areas beyond the programming language, or other programming aspects that could present security risks. Cryptographic tokens are emergent technologies, they carry high levels of technical risks and uncertainty. 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. This audit report could include false positives, false negatives, and other unpredictable results.

CONFIDENTIALITY

This report is subject to the terms and conditions (including without limitations, description of services, confidentiality, disclaimer and limitation of liability) outlined in the scope of the audit provided to the client. This report should not be transmitted, disclosed, referred to, or relied upon by any individual for any purpose without InterFi Network's prior written consent.

NO FINANCIAL ADVICE

This audit report does not indicate the endorsement of any particular project or team, nor guarantees its security. No third party should rely on the reports in any way, including to make any decisions to buy or sell a product, service or any other asset. The information provided in this report does not constitute investment advice, financial advice, trading advice, or any other sort of advice and you should not treat any of the report's content as such. This audit report should not be used in any way

to make decisions around investment or involvement. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort.

FOR AVOIDANCE OF DOUBT, SERVICES, INCLUDING ANY ASSOCIATED AUDIT REPORTS OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.

TECHNICAL DISCLAIMER

ALL SERVICES, AUDIT REPORTS, SMART CONTRACT AUDITS, OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF ARE PROVIDED "AS IS" AND "AS AVAILABLE" AND WITH ALL FAULTS AND DEFECTS WITHOUT WARRANTY OF ANY KIND. TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, VITAL BLOCK HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESSED, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO SERVICES, AUDIT REPORT, OR OTHER MATERIALS. WITHOUT LIMITING THE FOREGOING, VITAL BLOCK SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM THE COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

WITHOUT LIMITING THE FOREGOING, VITAL BLOCK MAKES NO WARRANTY OF ANY KIND THAT ALL SERVICES, AUDIT REPORTS, SMART CONTRACT AUDITS, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF, WILL MEET THE CLIENT'S OR ANY OTHER INDIVIDUAL'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULT, BE COMPATIBLE OR WORK WITH ANY SOFTWARE, SYSTEM, OR OTHER SERVICES, OR BE SECURE, ACCURATE, COMPLETE, FREE OF HARMFUL CODE, OR ERROR-FREE.

TIMELINESS OF CONTENT

The content contained in this audit report is subject to change without any prior notice. Vital Block does not guarantee or warrant the accuracy, timeliness, or completeness of any report you access using the internet or other means, and assumes no obligation to update any information following the publication.

LINKS TO OTHER WEBSITES

This audit report provides, through hypertext or other computer links, access to websites and social accounts operated by individuals other than Vital Block. Such hyperlinks are provided for your reference and convenience only and are the exclusive responsibility of such websites and social accounts owners. You agree that Vital block Security is not responsible for the content or operation of such websites and social accounts and that Vital Block shall have no liability to you or any other person or entity for the use of third-party websites and social accounts. You are solely responsible for determining the extent to which you may use any content at any other websites and social accounts to which you link from the report.

ABOUT VITAL BLOCK

Vital Block provides intelligent blockchain Security Solutions. We provide solidity and Raw Code Review, testing, and auditing services. We have Partnered with 15+ Crypto Launchpads, audited 50+ smart contracts, and analyzed 200,000+ code lines. We have worked on major public blockchains e.g., Ethereum, Binance, Cronos, Doge, Polygon, Avalanche, Metis, Fantom, Bitcoin Cash, Aptos, Oasis, etc.

Vital Block is Dedicated to Making Defi & Web3 A Safer Place. We are Powered by Security engineers, developers, UI experts, and blockchain enthusiasts. Our team currently consists of 5 core members, and 4+ casual contributors.

Website: https://Vitalblock.org

Email: info@vitalblock.org

GitHub: https://github.com/vital-block

Telegram (Engineering): https://t.me/vital_block

Telegram (Onboarding): https://t.me/vitalblock_cmo

vital-block

info@vitalblock.org

www.Vitalblock.org

Vital Block Dedicated to securing Public and Private Blockchain Ecosystem