expelee

Building the Futuristic Blockchain Ecosystem

SECURITY AUDIT REPORT

GOLD

TOKEN OVERVIEW

Risk Findings

Severity	Found
High	1
Medium	0
Low	0
Informational	1

Centralization Risks

Owner Privileges	Description
Can Owner Set Taxes >25% ?	Not Detected
Owner needs to enable trading ?	Not Detected
Can Owner Disable Trades ?	Not Detected
Can Owner Mint ?	Not Detected
Can Owner Blacklist ?	Not Detected
Can Owner set Max Wallet amount ?	Not Detected
Can Owner Set Max TX amount ?	Not Detected

expelee

TABLE OF CONTENTS

OVERVIEW

The Expelee team has performed a line-by-line manual analysis and automated review of the smart contract. The smart contract was analysed mainly for common smart contract vulnerabilities, exploits, and manipulation hacks. According to the smart contract audit:

Audit Result	**Passed**
KYC Verification	**-**
Audit Date	**29 July 2023**

CONTRACT DETAILS

Token Name: Gold Chain

Symbol: GOLD

Network: Ethereum

Language: Solidity

Contract Address:
0x8F3CA645A5902A176281ec032603Ad27D708112A

Total Supply:10,000,000,000

Owner's Wallet:
0x7E9C38A96f3E717d2344A2d977d8Afc3a4d18b5f

Deployer's Wallet:
0x7E9C38A96f3E717d2344A2d977d8Afc3a4d18b5f

Testnet.
https://testnet.bscscan.com/token/0x9Ab443F805A85Dc0982Aa2b19C452719456773e8

AUDIT METHODOLOGY

Audit Details

Our comprehensive audit report provides a full overview of the audited system's architecture, smart contract codebase, and details on any vulnerabilities found within the system.

Audit Goals

The audit goal is to ensure that the project is built to protect investors and users, preventing potentially catastrophic vulnerabilities after launch , that lead to scams and rugpulls.

Code Quality

Our analysis includes both automatic tests and manual code analysis for the following aspects:

- Exploits
- Back-doors
- Vulnerability
- Accuracy
- Readability

Tools

- DE
- Open Zeppelin
- Code Analyzer
- Solidity Code
- Compiler
- Hardhat

VULNERABILITY CHECKS

Design Logic	Passed
Compiler warnings	Passed
Private user data leaks	Passed
Timestamps dependence	Passed
Integer overflow and underflow	Passed
Race conditions & reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front Running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zepplin module	Passed

RISK CLASSIFICATION

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and acces control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

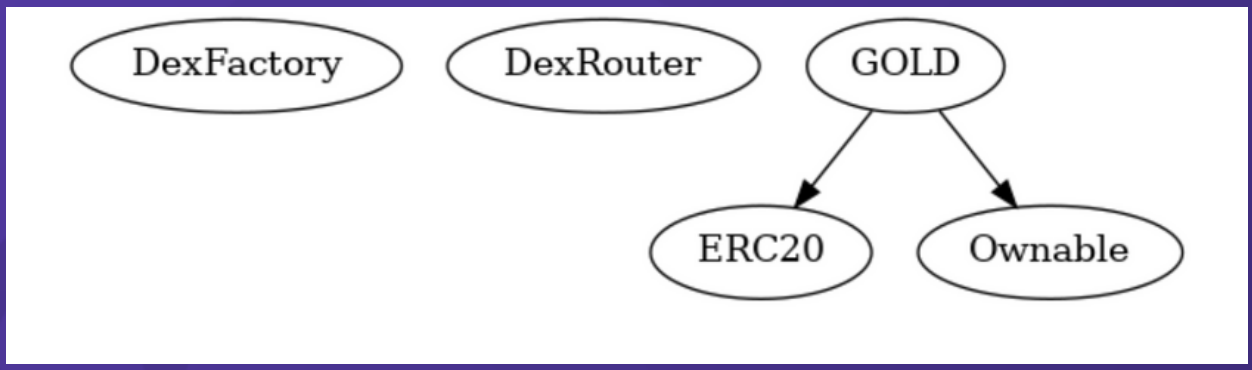
Issues on this level are minor details and warning that can remain unfixed.

Informational

Issues on this level are minor details and warning that can remain unfixed.

expelee

INHERITANCE TREES



FUNCTION DETAILS

Contract	Type	Bases		
└	**Function Name**	**Visibility**	**Mutability**	**Modifiers**
DexFactory	Interface			
└	createPair	External ❗	🛑	NO ❗
DexRouter	Interface			
└	factory	External ❗		NO ❗
└	WETH	External ❗		NO ❗
└	addLiquidityETH	External ❗	💵	NO ❗
└	swapExactTokensForETHSupportingFeeOnTransferTokens	External ❗	🛑	NO ❗
GOLD	Implementation	ERC20, Ownable		
└	<Constructor>	Public ❗	🛑	ERC20
└	setmarketingWallet	External ❗	🛑	onlyOwner
└	enableTrading	External ❗	🛑	onlyOwner
└	setSwapTokensAtAmount	External ❗	🛑	onlyOwner
└	toggleSwapping	External ❗	🛑	onlyOwner
└	setWhitelistStatus	External ❗	🛑	onlyOwner
└	checkWhitelist	External ❗		NO ❗
└	_takeTax	Internal 🔒	🛑	
└	_transfer	Internal 🔒	🛑	
└	internalSwap	Internal 🔒	🛑	
└	swapToETH	Internal 🔒	🛑	
└	withdrawStuckETH	External ❗	🛑	onlyOwner
└	withdrawStuckTokens	External ❗	🛑	onlyOwner
└	<Receive Ether>	External ❗	💵	NO ❗

FUNCTION DETAILS

Legend

Symbol	Meaning
🛑	Function can modify state
💵	Function is payable

TESTNET VERSION

Adding Liquidity ✅
Tx:
https://testnet.bscscan.com/tx/0x9625826bd30523c47735bd3efa2f9615fc668b711d33c8845ec54a5a3c0fb7f1

==========

Buying when excluded from fees ✅
Tx (0% tax):
https://testnet.bscscan.com/tx/0xab7e2ca9f4318461a40f01ac63bf4467cac12dd856786172a704877529ec2785

==========

Selling when excluded from fees ✅
Tx (0% tax):
https://testnet.bscscan.com/tx/0x2c58ec44455d1d57cdb2477c0b2181a35556e91fe7f9a0714909806a2569493e

==========

Transferring when excluded from fees ✅
Tx (0% tax):
https://testnet.bscscan.com/tx/0x23f53d540cf2abae569f8a546d26415b5f992bc82c0cfd7c0497106b702f841c

==========

Buying ✅
Tx (1% tax):
https://testnet.bscscan.com/tx/0x01e432c92b79cd2ec50fe8e51a64d1793f2f4fd87322d58dfdcf0d928b6ff7ee

TESTNET VERSION

Selling ✅
Tx (1% tax):
https://testnet.bscscan.com/tx/0x01e432c92b79cd2ec50fe8e51a64d1793f2f4fd87322d58dfdcf0d928b6ff7ee

==========

Transferring ✅
Tx(1% tax):
https://testnet.bscscan.com/tx/0x727dec0ab2b58f0a64f8d809c5d29cdb3e85d20c71bde962bd475a5e6ddde5cd

==========

Internal swap (BNB to marketing wallet | reward token to dividend tracker | reward distribution) ✅
Tx:
https://testnet.bscscan.com/address/0x4cc4fca718e3bdfe053efc0749cb64540248a725#internaltx

MANUAL REVIEW

Severity Criteria

Expelee assesses the severity of disclosed vulnerabilities according to methodology based on OWASP standarts.

Vulnerabilities are dividend into three primary risk categroies:
High
Medium
Low

High-level considerations for vulnerabilities span the following key areas when conducting assessments:

- Malicious input handling
- Escalation of privileges
- Arithmetic
- Gas use

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

HIGH RISK FINDING

Trades are disabled by default

Category: Centralization
Status: Resolved (Contract owned by safu developer)
Impact: High

Overview:
The contract has been structured such that all trading is disabled by default, necessitating the contract owner's manual intervention to enable trading. This can lead to a situation where, if trades remain disabled, token holders won't be able to buy, sell, or trade their tokens, causing a severe impact on the token's usability and market liquidity.

```
function enableTrading() external onlyOwner {
 require(!tradingEnabled, "Trading is already enabled");
 tradingEnabled = true;
 startTradingBlock = block.number;
}
```

Suggestion:
To mitigate this risk, it is recommended that trading be enabled before the token presale. This can be achieved by invoking the "startTrading" function or by transferring ownership of the contract to a third-party that has established trust with the community, such as a Certified SAFU developer. This reduces the concentration of power and the potential for malicious actions, thereby promoting a more decentralized and fair environment for all participants.

INFORMATINAL RISK FINDING

Internal swap could be disabled forever

Category: Logical
Status: Open
Impact: Informational

Overview:
internalSwap function returns if taxAmount is equal to 0 but it doesn not reset isSwapping to false. In this situation, isSwapping will always be “true’ which means internalSwap function wont be called again.
This issue is categorized as “informational’ since taxAmount is always greater than 0, however its still suggested to correct this issue.

```
function internalSwap() internal {
 isSwapping = true;
 uint256 taxAmount = balanceOf(address(this));
 if (taxAmount == 0) {
  return;
 }
 swapToETH(balanceOf(address(this)));
 (bool success, ) = marketingWallet.call{ value: address(this).balance }("");
 require(success, "Transfer failed.");
 isSwapping = false;
}
```

Suggestion:
Ensure to set isSwapping to “false’ under any conditions after internalSwap;

```
isSwapping = true;
internalSwap()
isSwapping = false
```

ABOUT EXPELEE

Expelee is a product-based aspirational Web3 start-up. Coping up with numerous solutions for blockchain security and constructing a Web3 ecosystem from deal making platform to developer hosting open platform, while also developing our own commercial and sustainable blockchain.

www.expelee.com

expeleeofficial
expelee
Expelee
expelee
expelee_official
expelee-co

expelee

Building the Futuristic Blockchain Ecosystem

DISCLAIMER

All the content provided in this document is for general information only and should not be used as financial advice or a reason to buy any investment. Team provides no guarantess against the sale of team tokens or the removal of liquidity by the project audited in this document.

Always do your own research and project yourselves from being scammed. The Expelee team has audited this project for general information and only expresses their opinion based on similar projects and checks from popular diagnostic tools.

Under no circumstances did Expelee receive a payment to manipulate those results or change the awarding badge that we will be adding in our website. Alway do your own research and protect yourselves from scams.

This document should not be presented as a reason to buy or not buy any particular token. The Expelee team disclaims any liability for the resulting losses.