Cyberscope

Audit Report

FrontFanz

May 2023

Network MATIC

Address 0xB8c601785D38067a8C0141Cb2bA2F0c7b060075B

Audited by © cyberscope

Analysis

Critical Medium Minor / Informative Pass

Severity	Code	Description	Status
	ST	Stops Transactions	Passed
	OCTD	Transfers Contract's Tokens	Passed
	OTUT	Transfers User's Tokens	Passed
	ELFM	Exceeds Fees Limit	Passed
	ULTW	Transfers Liquidity to Team Wallet	Passed
	MT	Mints Tokens	Passed
	BT	Burns Tokens	Passed
	BC	Blacklists Addresses	Passed

Diagnostics

Critical Medium Minor / Informative

Severity	Code	Description	Status
	L19	Stable Compiler Version	Unresolved

Table of Contents

Analysis 1
Diagnostics 2
Table of Contents 3
Review 4
Audit Updates 4
Source Files 5
Findings Breakdown 6
L19 - Stable Compiler Version 7
Description 7
Recommendation 7
Functions Analysis 8
Inheritance Graph 11
Flow Graph 12
Summary 13
Disclaimer 14
About Cyberscope 15

Review

Contract Name	Token
Compiler Version	v0.8.18+commit.87f61d96
Optimization	200 runs
Explorer	https://polygonscan.com/address/0xb8c601785d38067a8c0141cb2ba2f0c7b060075b
Address	0xb8c601785d38067a8c0141cb2ba2f0c7b060075b
Network	MATIC
Symbol	FANX
Decimals	18
Total Supply	1,000,000,000

Audit Updates

Initial Audit	05 Nov 2022 https://github.com/cyberscope-io/audits/blob/main/fanz/v1/audit.pdf
Corrected Phase 1	30 May 2023

Source Files

Filename	SHA256

Token.sol	103a22af529ced4e89c732be3a3b8d8d846cfcf1f05ad8d5faf9ede1e2debca9

Findings Breakdown



Critical	0
Medium	0
Minor / Informative	1

Severity	Unresolved	Acknowledged	Resolved	Other
Critical	0	0	0	0
Medium	0	0	0	0
Minor / Informative	1	0	0	0

L19 - Stable Compiler Version

Criticality	Minor / Informative
Location	Token.sol#L3
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 ^0.8.0;
```

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.

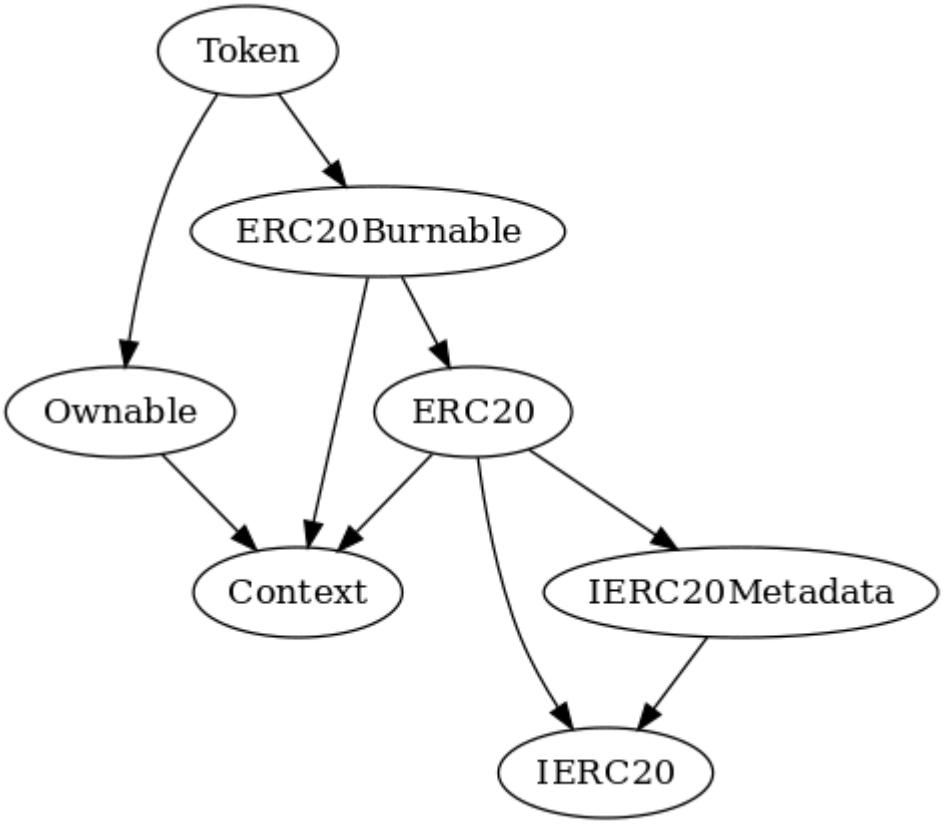
Functions Analysis

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
IERC20Metadata	Interface	IERC20		
	name	External		-
	symbol	External		-
	decimals	External		-
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
Ownable	Implementation	Context		

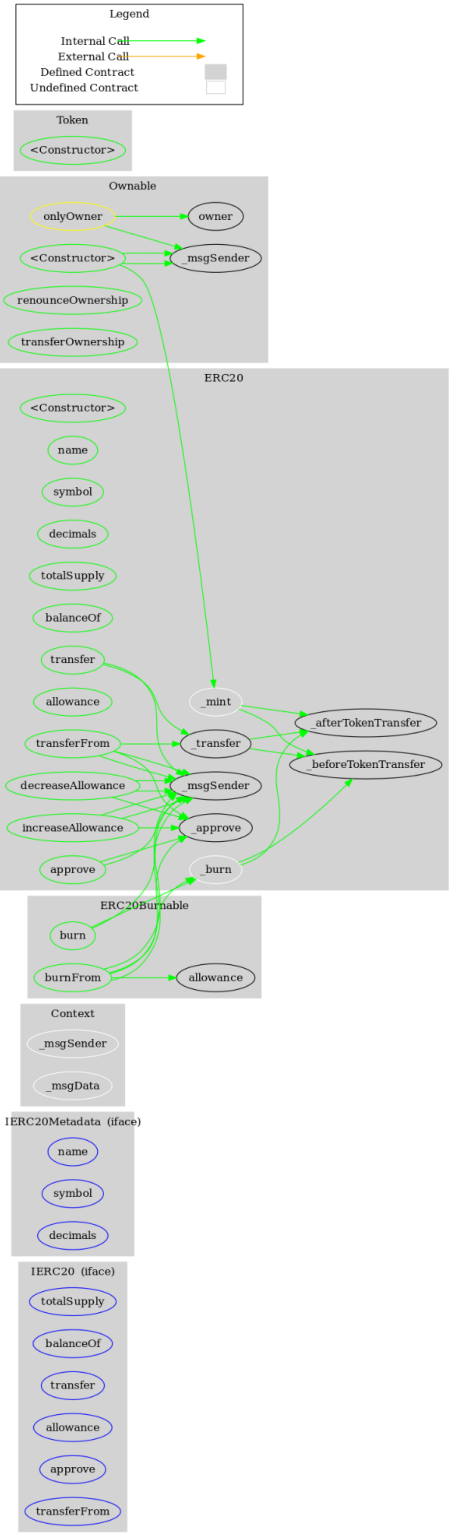
		Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
ERC20	Implementation	Context, IERC20, IERC20Metadata		
		Public	✓	-
	name	Public		-
	symbol	Public		-
	decimals	Public		-
	totalSupply	Public		-
	balanceOf	Public		-
	transfer	Public	✓	-
	allowance	Public		-
	approve	Public	✓	-
	transferFrom	Public	✓	-
	increaseAllowance	Public	✓	-
	decreaseAllowance	Public	✓	-
	_transfer	Internal	✓	
	_mint	Internal	✓	
	_burn	Internal	✓	
	_approve	Internal	✓	

	_beforeTokenTransfer	Internal	✓	
	_afterTokenTransfer	Internal	✓	
ERC20Burnable	Implementation	Context, ERC20		
	burn	Public	✓	-
	burnFrom	Public	✓	-
Token	Implementation	ERC20Burnable, Ownable		
		Public	✓	ERC20

Inheritance Graph



Flow Graph


Legend
Internal Call
External Call
Defined Contract
Undefined Contract
Token
<Constructor>
Ownable
onlyOwner
owner
<Constructor>
msgSender
renounceOwnership
transferOwnership
ERC20
<Constructor>
name
symbol
decimals
totalSupply
balanceOf
transfer
allowance
_mint
_afterTokenTransfer
transferFrom
_transfer
_beforeTokenTransfer
decreaseAllowance
msgSender
increaseAllowance
_approve
approve
_burn
ERC20Burnable
burn
burnFrom
allowance
Context
_msgSender
_msgData
IERC20Metadata (iface)
name
symbol
decimals
IERC20 (iface)
totalSupply
balanceOf
transfer
allowance
approve
transferFrom

Summary

FrontFanz contract implements a token mechanism. This audit investigates security issues, business logic concerns, and potential improvements. FrontFanz is an interesting project that has a friendly and growing community. The Smart Contract analysis reported no compiler errors or critical issues. The Contract Owner can access some admin functions that can not be used in a malicious way to disturb the users' transactions.

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

Cyberscope

Audit Report

FrontFanz

November 2022

Type	ERC20
Network	MATIC
Address	0x124C31a823CDf7CD391aDAEE4aA32455eB3E76Ca
Audited by	© cyberscope

Table of Contents

Table of Contents 1
Contract Review 2
Source Files 2
Audit Updates 2
Contract Roles 3
Contract Analysis 4
Contract Diagnostics 5
L04 - Conformance to Solidity Naming Conventions 6
Description 6
Recommendation 6
L15 - Local Scope Variable Shadowing 7
Description 7
Recommendation 7
Contract Functions 8
Contract Flow 11
Domain Info 12
Summary 13
Disclaimer 14
About Cyberscope 15

Contract Review

Contract Name	FrontFanz
Compiler Version	v0.8.7+commit.e28d00a7
Optimization	200 runs
Licence	None
Explorer	https://polygonscan.com/token/0x124C31a823CDf7CD391aDAEE4aA32455eB3E76Ca
Symbol	FANZ
Decimals	18
Total Supply	500,000,000
Domain	frontfanz.com

Source Files

Filename	SHA256
contract.sol	9c2a9c6d3d56bc528b6e3d259bfcd3ec27d3ccbcb930b9062023810355e7e194

Audit Updates

Initial Audit	5th November 2022
Corrected	

Contract Roles

The contract contains a mint and a blacklisting functionality but it has renounced the ownership. Hence the abovementioned functionalities are not effective anymore.

Renounce of mint role

https://polygonscan.com/tx/0xb53094388ea9655a1bf3fb7217538b217e623d5c5e52ad2eac8845fe017ea4a7

Renounce of blacklist role

https://polygonscan.com/tx/0x2f00af3621c399a64b69196a0d6b5ae240c7bb10ae4f4e75ed1fd50b5c1ab282

Renounce of contract owner

https://polygonscan.com/tx/0xdc98f5ec41e838f597d4d145beb20caa70da089f6294191abfd5ef92d7af9831

Contract Analysis

● Critical ● Medium ● Minor / Informative ● Pass

Severity	Code	Description	Status
●	ST	Stops Transactions	Passed
●	OCTD	Transfers Contract's Tokens	Passed
●	OTUT	Transfers User's Tokens	Passed
●	ELFM	Exceeds Fees Limit	Passed
●	ULTW	Transfers Liquidity to Team Wallet	Passed
●	MT	Mints Tokens	Passed
●	BT	Burns Tokens	Passed
●	BC	Blacklists Addresses	Passed

Contract Diagnostics

Critical Medium Minor / Informative

Severity	Code	Description	Status
	L04	Conformance to Solidity Naming Conventions	Unresolved
	L15	Local Scope Variable Shadowing	Unresolved

L04 - Conformance to Solidity Naming Conventions

Criticality	minor / informative
Location	contract.sol#L826,881,840,818,892,835
Status	Unresolved

Description

Solidity defines a naming convention that should be followed. Rule exceptions:

- Allow constant variable name/symbol/decimals to be lowercase.
- Allow _ at the beginning of the mixed_case match for private variables and unused parameters.

```
_account
_amount
_newBlacklister
_newMinter
_to
```

Recommendation

Follow the Solidity naming convention.
https://docs.soliditylang.org/en/v0.4.25/style-guide.html#naming-conventions.

L15 - Local Scope Variable Shadowing

Criticality	minor / informative
Location	contract.sol#L858
Status	Unresolved

Description

The are variables that are defined in the local scope containing the same name from an upper scope.

```
_name
_symbol
```

Recommendation

The local variables should have different names from the upper scoped variables.

Contract Functions

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
IERC20Metadata	Interface	IERC20		
	name	External		-
	symbol	External		-
	decimals	External		-
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
SafeMath	Library			
	tryAdd	Internal		
	trySub	Internal		
	tryMul	Internal		
	tryDiv	Internal		
	tryMod	Internal		
	add	Internal		
	sub	Internal		
	mul	Internal		
	div	Internal		
	mod	Internal		

	sub	Internal		
	div	Internal		
	mod	Internal		
Ownable	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
ERC20	Implementation	Context, IERC20, IERC20Metadata		
	<Constructor>	Public	✓	-
	name	Public		-
	symbol	Public		-
	decimals	Public		-
	totalSupply	Public		-
	balanceOf	Public		-
	transfer	Public	✓	-
	allowance	Public		-
	approve	Public	✓	-
	transferFrom	Public	✓	-
	increaseAllowance	Public	✓	-
	decreaseAllowance	Public	✓	-
	_transfer	Internal	✓	
	_mint	Internal	✓	
	_burn	Internal	✓	
	_approve	Internal	✓	
	_beforeTokenTransfer	Internal	✓	
	_afterTokenTransfer	Internal	✓	
ERC20Burnable	Implementation	Context, ERC20		
	burn	Public	✓	-
	burnFrom	Public	✓	-

Blacklistable	Implementation	Ownable		
	isBlacklisted	External		-
	blacklist	External	✓	onlyBlacklister
	unBlacklist	External	✓	onlyBlacklister
	updateBlacklister	External	✓	onlyOwner
FrontFanz	Implementation	ERC20Burnable, Blacklistable		
	<Constructor>	Public	✓	ERC20
	mint	Public	✓	onlyMinter notBlacklisted notBlacklisted
	updateMinter	External	✓	onlyOwner
	approve	Public	✓	notBlacklisted notBlacklisted
	transferFrom	Public	✓	notBlacklisted notBlacklisted notBlacklisted
	transfer	Public	✓	notBlacklisted notBlacklisted

Contract Flow



Domain Info

Domain Name	frontfanz.com
Registry Domain ID	2640246655_DOMAIN_COM-VRSN
Creation Date	2021-09-11T04:06:29Z
Updated Date	2022-09-12T06:00:22Z
Registry Expiry Date	2023-09-11T04:06:29Z
Registrar WHOIS Server	whois.godaddy.com
Registrar URL	https://www.godaddy.com
Registrar	GoDaddy.com, LLC
Registrar IANA ID	146

The domain was created about 1 year before the creation of the audit. It will expire in 10 months.

There is no public billing information, the creator is protected by the privacy settings.

Summary

FrontFanz is an interesting project that has a friendly and growing community. The Smart Contract analysis reported no compiler error or critical issues. The contract Owner can access some admin functions that can not be used in a malicious way to disturb the users' transactions.

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.

Cyberscope team provides no guarantees against the sale of team tokens or the removal of liquidity by the project audited in this document. Always Do your own research and protect yourselves from being scammed.

The Cyberscope 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 Cyberscope receive a payment to manipulate those results or change the awarding badge that we will be adding in our website.

Always 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 Cyberscope team disclaims any liability for the resulting losses.

About Cyberscope

Coinscope audit and K.Y.C. service has been rebranded to Cyberscope.

Coinscope is the leading early coin listing, voting and auditing authority firm. The audit process is analyzing and monitoring many aspects of the project. That way, it gives the community a good sense of security using an informative report and a generic score.

Cyberscope and Coinscope are aiming to make crypto discoverable and efficient globally. They provide all the essential tools to assist users draw their own conclusions.



The Cyberscope team

https://www.cyberscope.io