Cyberscope

A TAC Security Company

Audit Report

APFC Token

November 2025

Network ETH

Address 0x8ed955a2b7d2c3a17a9d05daca95e01818f8c11e

Audited by © cyberscope

Analysis

Critical Medium Minor / Informative Pass

Severity	Code	Description	Status
●	ST	Stops Transactions	Passed
●	OTUT	Transfers User's Tokens	Passed
●	ELFM	Exceeds Fees Limit	Passed
●	MT	Mints Tokens	Passed
●	BT	Burns Tokens	Passed
●	BC	Blacklists Addresses	Passed

Diagnostics

Critical Medium Minor / Informative

Severity	Code	Description	Status
	MEM	Missing Error Messages	Unresolved
	DSV	Deprecated Solidity Version	Unresolved

Table of Contents

Risk Classification

The criticality of findings in Cyberscope's smart contract audits is determined by evaluating multiple variables. The two primary variables are:

1. **Likelihood of Exploitation**: This considers how easily an attack can be executed, including the economic feasibility for an attacker.
2. **Impact of Exploitation**: This assesses the potential consequences of an attack, particularly in terms of the loss of funds or disruption to the contract's functionality.

Based on these variables, findings are categorized into the following severity levels:

1. **Critical**: Indicates a vulnerability that is both highly likely to be exploited and can result in significant fund loss or severe disruption. Immediate action is required to address these issues.
2. **Medium**: Refers to vulnerabilities that are either less likely to be exploited or would have a moderate impact if exploited. These issues should be addressed in due course to ensure overall contract security.
3. **Minor**: Involves vulnerabilities that are unlikely to be exploited and would have a minor impact. These findings should still be considered for resolution to maintain best practices in security.
4. **Informative**: Points out potential improvements or informational notes that do not pose an immediate risk. Addressing these can enhance the overall quality and robustness of the contract.

Severity	Likelihood / Impact of Exploitation
Critical	Highly Likely / High Impact
Medium	Less Likely / High Impact or Highly Likely/ Lower Impact
Minor / Informative	Unlikely / Low to no Impact

Review

Contract Name	APFC
Compiler Version	v0.4.24+commit.e67f0147
Optimization	200 runs
Explorer	https://etherscan.io/address/0x8ed955a2b7d2c3a17a9d05daca95e01818f8c11e
Address	0x8ed955a2b7d2c3a17a9d05daca95e01818f8c11e
Network	ETH
Symbol	APFC
Decimals	18
Total Supply	250,000,000

Audit Updates

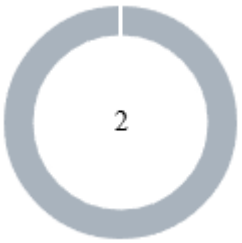
Initial Audit	07 Nov 2025

Source Files

Filename	SHA256
StandardToken.sol	17f3420015158148d711851a1f8a266ca417d25645f8ad37569ed9ba34ad351b
SafeMath.sol	2992be99ec79983fab97b08158bbad475f55e02ec8c5293d663fa124a9b75c66
Ownable.sol	35feff96ea2ff782dfa0d35815b2d394cff31bbb2270b77aab4abac1bf6e4b9b

MintableToken.sol	17bd054d51a9da8a42e807a30e4da006b3ce6b57212b773f1001ac0c9abb707d
ERC20Basic.sol	8f09e53364787fdff9a9f701c4c5c35b8786d26aed5cce84ca460cd854e8a130
ERC20.sol	1570b37daa43d61c3f045639f96f63ca687ac0a8444ff944cd1ed1c33c0141e9
CappedToken.sol	c937963bb37204634a4380d6a508728463a219f0c5334e20c765602ecbab4846
CapToken.sol	73473c69b45058870c7ce6b3db6876a3bef5450e69c23d27361ec811d81ae781
BasicToken.sol	dde32d0bba9da74c52e0710e431996308e472f2b07d468c69609e17a3c082e0a

Findings Breakdown



Critical	0
Medium	0
Minor / Informative	2

Severity	Unresolved	Acknowledged	Resolved	Other
Critical	0	0	0	0
Medium	0	0	0	0
Minor / Informative	2	0	0	0

MEM - Missing Error Messages

Criticality	Minor / Informative
Location	StandardToken.sol#L33,34,35 Ownable.sol#L32,60 MintableToken.sol#L20,25 CappedToken.sol#L15,32 BasicToken.sol#L32,33
Status	Unresolved

Description

The contract is missing error messages. Specifically, there are no error messages to 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.

```
Shell
require(_value <= balances[_from])
require(_value <= allowed[_from][msg.sender])
require(_to != address(0))
require(msg.sender == owner)
require(_newOwner != address(0))
require(!mintingFinished)
require(_cap > 0)
require(totalSupply_.add(_amount) <= cap)
require(_value <= balances[msg.sender])
```

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.

DSV - Deprecated Solidity Version

Criticality	Minor / Informative
Location	CapToken.sol#L1
Status	Unresolved

Description

The contracts are written using Solidity version ^0.4.24, which is deprecated and no longer maintained by the Solidity development team. Relying on outdated compiler versions can expose the codebase to known vulnerabilities, unresolved bugs, and missed performance improvements. This may compromise the security, efficiency, and long-term maintainability of the contracts.

```
Shell
pragma solidity ^0.4.24;
```

Recommendation

The team is advised to migrate the contracts to a recent, stable, and supported Solidity version. This ensures access to the latest compiler optimizations and built-in security features, such as native protection against integer overflows and underflows, enhancing both performance and safety.

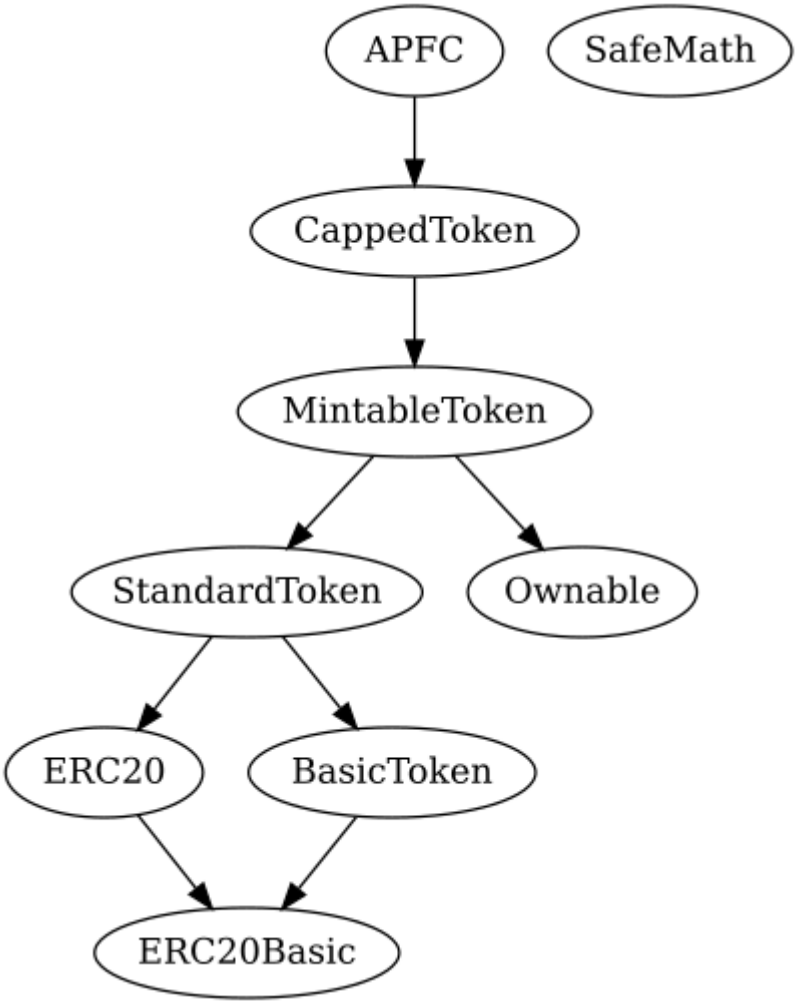
Functions Analysis

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
StandardToken	Implementation	ERC20, BasicToken		
	transferFrom	Public	✓	-
	approve	Public	✓	-
	allowance	Public		-
	increaseApproval	Public	✓	-
	decreaseApproval	Public	✓	-
SafeMath	Library			
	mul	Internal		
	div	Internal		
	sub	Internal		
	add	Internal		
Ownable	Implementation			
		Public	✓	-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	_transferOwnership	Internal	✓	

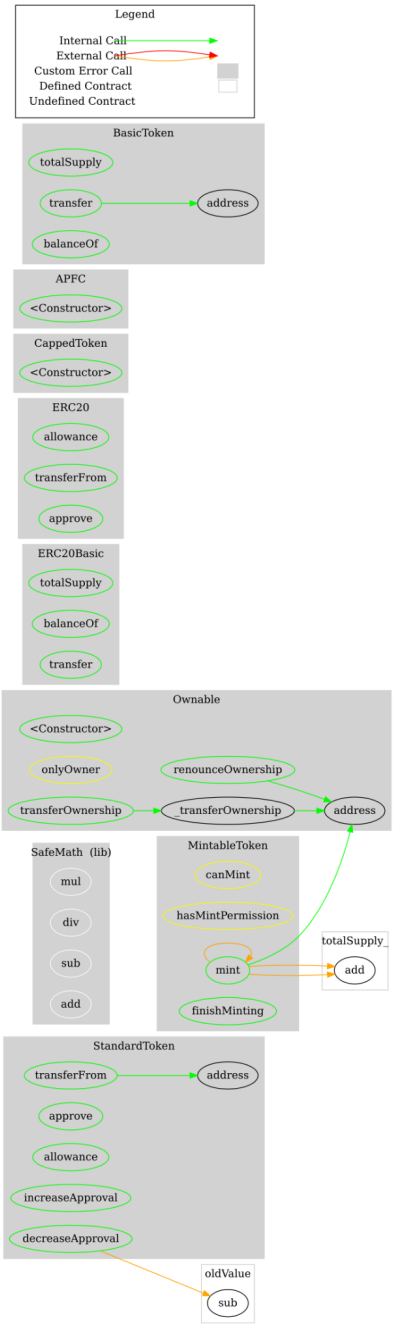
MintableToken	Implementation	StandardToken, Ownable		
	mint	Public	✓	hasMintPermission canMint
	finishMinting	Public	✓	onlyOwner canMint
ERC20Basic	Implementation			
	totalSupply	Public		-
	balanceOf	Public		-
	transfer	Public	✓	-
ERC20	Implementation	ERC20Basic		
	allowance	Public		-
	transferFrom	Public	✓	-
	approve	Public	✓	-
CappedToken	Implementation	MintableToken		
		Public	✓	-
	mint	Public	✓	-
APFC	Implementation	CappedToken		
		Public	✓	CappedToken
BasicToken	Implementation	ERC20Basic		
	totalSupply	Public		-

	transfer	Public	✓	-
	balanceOf	Public		-

Inheritance Graph



Flow Graph


Legend
Internal Call
External Call
Custom Error Call
Defined Contract
Undefined Contract
BasicToken
totalSupply
transfer
address
balanceOf
APFC
<Constructor>
CappedToken
<Constructor>
ERC20
allowance
transferFrom
approve
ERC20Basic
totalSupply
balanceOf
transfer
Ownable
<Constructor>
onlyOwner
renounceOwnership
transferOwnership
transferOwnership
address
SafeMath (lib)
mul
div
sub
add
MintableToken
canMint
hasMintPermission
mint
finishMinting
totalSupply_
add
StandardToken
transferFrom
address
approve
allowance
increaseApproval
decreaseApproval
oldValue
sub

Summary

APF Coin contract implements a token mechanism. This audit investigates security issues, business logic concerns and potential improvements. APF Coin 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

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 TAC 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.

A **TAC Security** Company

The Cyberscope team

cyberscope.io