Cyberscope

Audit Report

Safereum

September 2023

Network	ETH
Address	0xd29A96Dc9e7e14e9F8Ff6C9c96EFA503a2fD4577
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
●	RFO	Redundant Function Overrides	Unresolved
●	CO	Constructor Optimization	Unresolved

Table of Contents

Review

Contract Name	Safereum
Compiler Version	v0.8.19+commit.7dd6d404
Optimization	200 runs
Explorer	https://etherscan.io/address/0xd29a96dc9e7e14e9f8ff6c9c96efa503a2fd4577
Address	0xd29a96dc9e7e14e9f8ff6c9c96efa503a2fd4577
Network	ETH
Symbol	SAFEREUM
Decimals	18
Total Supply	1,000,000,000,000

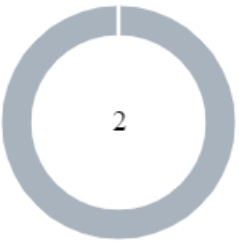
Audit Updates

Initial Audit	26 Sep 2023

Source Files

Filename	SHA256
Token.sol	353c81e441bcfa1e4e5c68430e751a30880a036234a319b1cfb42ca9d8b4d20e
Ownable.sol	33422e7771fefe5fbfe8934837515097119d82a50eda0e49b38e4d6a64a1c25d
IERC20Metadata.sol	b10e2f8bcc3ed53a5d9a82a29b1ad3209225331bb4de4a0459862a762cf83a1a
IERC20.sol	7ebde70853ccafcf1876900dad458f46eb9444d591d39bfc58e952e2582f5587
ERC20Burnable.sol	480b22ce348050fdb85a693e38ed6b4767a94e4776fc6806d6808a0ec171177e
ERC20.sol	f70c6ae5f2dda91a37e17cfcbec390cc59515ed0d34e316f036f5431b5c0a3f2
Context.sol	1458c260d010a08e4c20a4a517882259a23a4baa0b5bd9add9fb6d6a1549814a

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

RFO - Redundant Function Overrides

Criticality	Minor / Informative
Location	Token.sol#L26,30,37
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.

The contract overrides the following functions without changing the default function definition. Hence, the overrides are redundant.

```
function decimals() public pure override returns (uint8) {
    return 18;
}

function _beforeTokenTransfer(address from, address to, uint256 amount)
    internal
    override
{
    super._beforeTokenTransfer(from, to, amount);
}

function _afterTokenTransfer(address from, address to, uint256 amount)
    internal
    override
{
    super._afterTokenTransfer(from, to, amount);
}
```

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.

CO - Constructor Optimization

Criticality	Minor / Informative
Location	Token.sol#L18
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.

The contract does not employ the `supplyRecipient` variable in the `_transferOwnership` method call. Instead, it reassigns the address directly.

```
constructor()
    ERC20(unicode"Safereum", unicode"SAFEREUM")
{
    address supplyRecipient =
0x67c8423a7709aDB8ED31c04DcbB0C161637b807F;

    _mint(supplyRecipient, 10000000000000 * (10 ** decimals()) / 10);
    _transferOwnership(0x67c8423a7709aDB8ED31c04DcbB0C161637b807F);
}
```

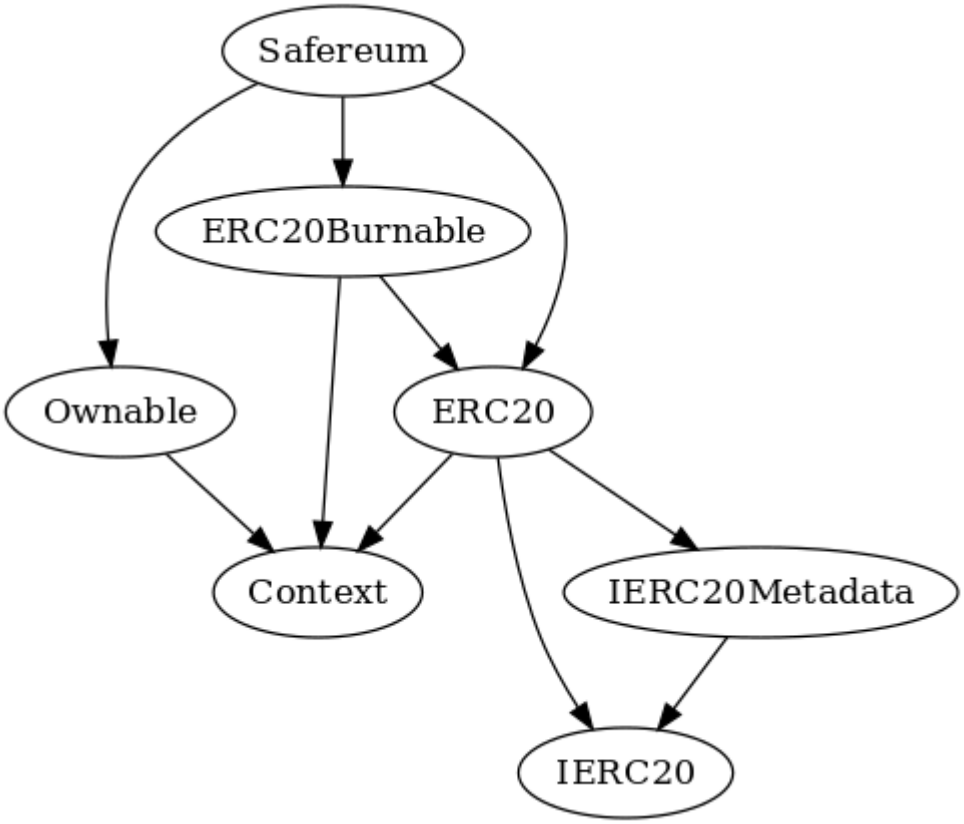
Recommendation

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 reuse the `supplyRecipient` variable.

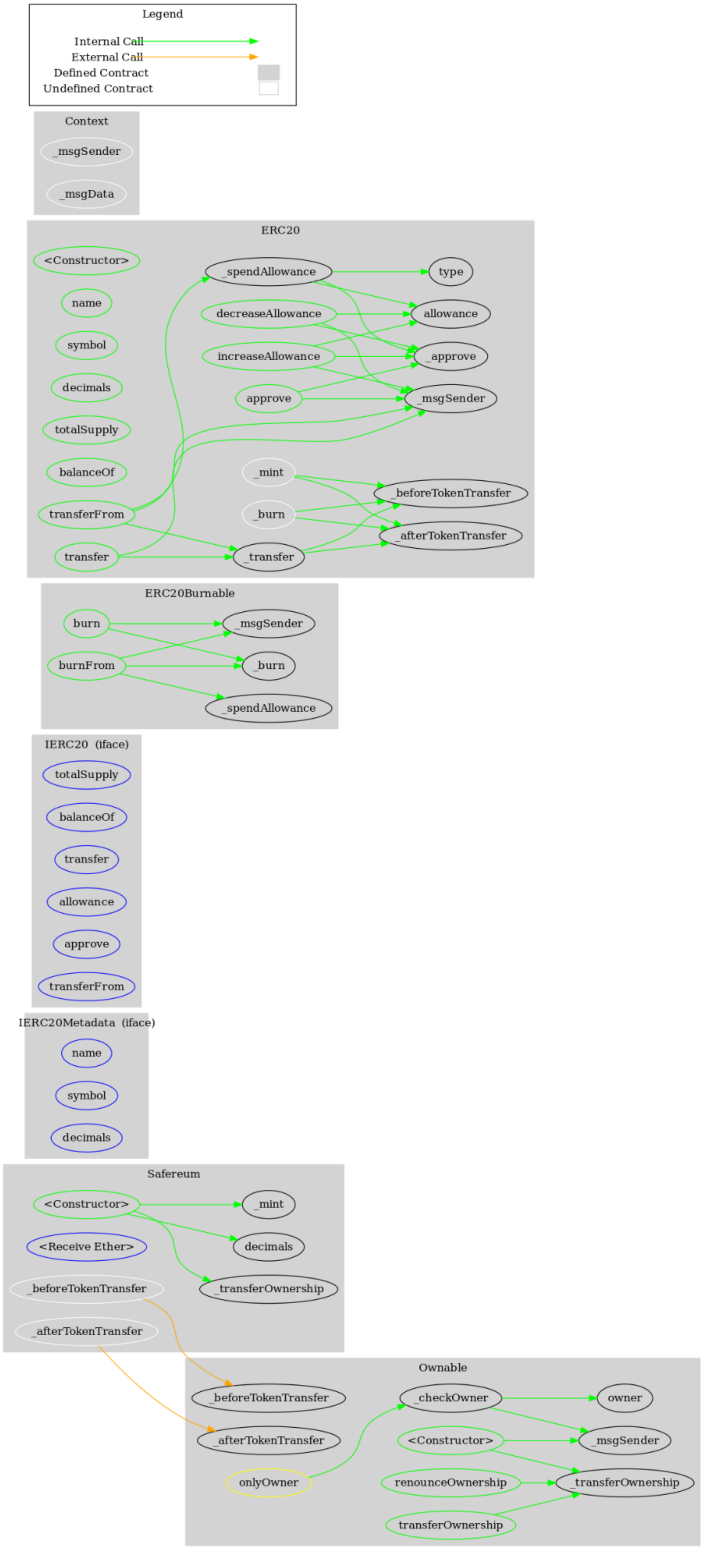
Functions Analysis

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
Safereum	Implementation	ERC20, ERC20Burnable, Ownable		
		Public	✓	ERC20
		External	Payable	-
	decimals	Public		-
	_beforeTokenTransfer	Internal	✓	
	_afterTokenTransfer	Internal	✓	

Inheritance Graph



Flow Graph


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

Summary

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