Cyberscope

Audit Report

AI MASA

July 2023

Network BSC Testnet

Address 0x68A8152720df8724617c68Bfe913cAC509335fea

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	Unresolved
●	BT	Burns Tokens	Passed
●	BC	Blacklists Addresses	Passed

Diagnostics

● Critical ● Medium ● Minor / Informative

Severity	Code	Description	Status
●	PFM	Potential Functions Misuse	Unresolved
●	L19	Stable Compiler Version	Unresolved

Table of Contents

Review

Explorer	https://testnet.bscscan.com/address/0x68a8152720df8724617c68bfe913cac509335fea

Audit Updates

Initial Audit	19 Jul 2023 https://github.com/cyberscope-io/audits/blob/main/masa/v1/audit.pdf
Corrected Phase 2	28 Jul 2023

Source Files

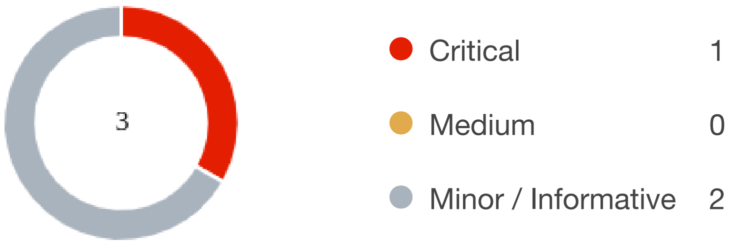
Filename	SHA256
contracts/token1.sol	b86a53023aae7ca8cc8826d4f21f50b66356fce5b15801aaf65db289b74ba287
@openzeppelin/contracts-upgradeable/utils/StringsUpgradeable.sol	357c8d1a0fb673fa10a884d6e27b383171ecc3eaf8dee8211de75f88ff77843d
@openzeppelin/contracts-upgradeable/utils/StorageSlotUpgradeable.sol	5b478023a1200e1364308ca06cdefec7cb7ab990a1cb904cbbdbaa7ba85076be
@openzeppelin/contracts-upgradeable/utils/CountersUpgradeable.sol	5c1ac829a429b0c2ca9b4c9ed8b78d412320e9175e45f088c4e9056ef95fbf21

@openzeppelin/contracts-upgradeable/utils/ContextUpgradeable.sol	5fb301961e45cb482fe4e05646d2f529aa449fe0e90c6671475d6a32356fa2d4
@openzeppelin/contracts-upgradeable/utils/AddressUpgradeable.sol	db92fc1b515decad3a783b1422190877d2d70b907c6e36fb0998d9465aee42db
@openzeppelin/contracts-upgradeable/utils/math/SignedMathUpgradeable.sol	4f06981f993ea4a96e078c2036b5a42e1edade38996e5180171d5fe4be2f18fe
@openzeppelin/contracts-upgradeable/utils/math/SafeCastUpgradeable.sol	647d03e70d45c15cd9aa3afc3b32de945ec024a022614e263f33bb35c557ac94
@openzeppelin/contracts-upgradeable/utils/math/MathUpgradeable.sol	fbf7ebc0f3c2cf5aef908ecce85e69af53db4e2c6652f61c8ac1e3f416c2fa99
@openzeppelin/contracts-upgradeable/utils/cryptography/EIP712Upgradeable.sol	ed30d96d25a360d320a807157db07b5bbb73392745ce8188b775787eb2d33fb9
@openzeppelin/contracts-upgradeable/utils/cryptography/ECDSAUpgradeable.sol	aefb3039d0aae994ad64c397dfa0bcc1ab6e675e2fd97b2fdfc0e7739def0b5b
@openzeppelin/contracts-upgradeable/token/ERC20/IERC20Upgradeable.sol	78a6bc84bbb417f0d8a6b12e181e0f783151774f4f0c054c5d3f920e70d69f8c
@openzeppelin/contracts-upgradeable/token/ERC20/ERC20Upgradeable.sol	9619cf23b549a5126042a4e20b09a2eb12dc8c2975258e3b8cde79cc593b6926
@openzeppelin/contracts-upgradeable/token/ERC20/extensions/draft-ERC20PermitUpgradeable.sol	a08be4078da127929eb0d760949376defa730f6af97f022822399b0ad880ad03
@openzeppelin/contracts-upgradeable/token/ERC20/extensions/IERC20PermitUpgradeable.sol	cf0f8a5ee1c560ad1c5b0847a1531c5904cee45d0ec811cd83d0d95cbd5a333b

@openzeppelin/contracts-upgradeable/token/ERC20/extensions/IERC20MetadataUpgradeable.sol	68bcca423fc72ec9625e219c9e36306c726a347e43f3711467c579bd3f6500c8
@openzeppelin/contracts-upgradeable/token/ERC20/extensions/ERC20VotesUpgradeable.sol	b89e9ae4dcbdd5b05db7ef2c7ee993f416d03b0787e613c33324dc480a65bbc0
@openzeppelin/contracts-upgradeable/token/ERC20/extensions/ERC20PermitUpgradeable.sol	dbd6de9e5c4479ed83e3106f5e1d03ed91a4d37e97b24e65e345366ec879d979
@openzeppelin/contracts-upgradeable/token/ERC20/extensions/ERC20BurnableUpgradeable.sol	ca660e828b0c4be205a9f56f3b87b91c1fa67cfd0f6e9dbd431faea7a6280d36
@openzeppelin/contracts-upgradeable/proxy/utils/UUPSUpgradeable.sol	04338003a3be8f5f38595048b591d80fdc147bf95cc7c6285e1e1a5f1afa2b47
@openzeppelin/contracts-upgradeable/proxy/utils/Initializable.sol	a2c4e5c274a586f145d278293ae33198cd8f412ab7e6d26f2394c8949b32b24b
@openzeppelin/contracts-upgradeable/proxy/beacon/IBeaconUpgradeable.sol	e0ac7115916f0dce0a8e80769694736f3e674bdc5b2e5853964c82004b1e1cc5
@openzeppelin/contracts-upgradeable/proxy/ERC1967/ERC1967UpgradeUpgradeable.sol	40dd5b14a370eea51ba94eb1b66a89638c6c54d86cc9f406599075c273e5e4c6
@openzeppelin/contracts-upgradeable/interfaces/draft-IERC1822Upgradeable.sol	a94576fd98585c07b2a9725f7c89c910a3a1909a03f49ec2df465327c6a0ffc3
@openzeppelin/contracts-upgradeable/interfaces/IERC6372Upgradeable.sol	a651c2fe286001386424f9ee592ffe45d8675d3512cce47e4274b587f4794772
@openzeppelin/contracts-upgradeable/interfaces/IERC5805Upgradeable.sol	ae6f56560f3313a609ab2878ead6ec287d27615c4d258194c244cceeeedd3ee3

@openzeppelin/contracts-upgradeable/interfaces/IERC5267Upgradeable.sol	6a0d92d0222dd70cdc073029b6fe979e03e65d9c9ea4f2b8ffb774e144d2a51e
@openzeppelin/contracts-upgradeable/interfaces/IERC1967Upgradeable.sol	167828e6f725b1d47d82bc912fd0f1c6ed0fb67a4e5e06a4d62e72b4a53e95cf
@openzeppelin/contracts-upgradeable/governance/utils/IVotesUpgradeable.sol	f1546747e3834205ca3358625f8a8e1de2e17912b94d0c3c9703a6a57e93d0b4
@openzeppelin/contracts-upgradeable/access/OwnableUpgradeable.sol	1fbf2a131b895514f0027866cc0deff151ea16424b4aed2b8c573d2275cfa9e8

Findings Breakdown



Severity	Unresolved	Acknowledged	Resolved	Other
● Critical	1	0	0	0
● Medium	0	0	0	0
● Minor / Informative	2	0	0	0

MT - Mints Tokens

Criticality	Critical
Location	contracts/token1.sol#L36
Status	Unresolved

Description

The contract owner has the authority to mint tokens. The owner may take advantage of it by calling the `mint` function. As a result, the contract tokens will be highly inflated.

```
function mint(address to, uint256 amount) public onlyOwner {
        _mint(to, amount);
  }
```

Recommendation

The team should carefully manage the private keys of the owner's account. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the contract admin functions. Some suggestions are:

- Introduce a time-locker mechanism with a reasonable delay.
- Introduce a multi-sign wallet so that many addresses will confirm the action.
- Introduce a governance model where users will vote about the actions.
- Renouncing the ownership will eliminate the threats but it is non-reversible.

PFM - Potential Functions Misuse

Criticality	Minor / Informative
Location	contracts/UUPSUpgradeable.sol#L74,89
Status	Unresolved

Description

The contract contains the `upgradeTo` and `upgradeToAndCall` functions that facilitate the upgradeability of the proxy's implementation. While these functions are essential for maintaining and improving the contract over time, there exists a potential risk. If these functions misused, they could redirect the proxy to point to a malicious or unintended implementation. Such a scenario could compromise the contract's intended behavior, potentially leading to loss of funds, unauthorized access, or unintended fuctionalities.

```
   function upgradeTo(address newImplementation) external
virtual onlyProxy {
        _authorizeUpgrade(newImplementation);
        _upgradeToAndCallUUPS(newImplementation, new bytes(0),
false);
    }

    function upgradeToAndCall(address newImplementation, bytes
memory data) external payable virtual onlyProxy {
        _authorizeUpgrade(newImplementation);
        _upgradeToAndCallUUPS(newImplementation, data, true);
    }
```

Recommendation

It is recommended to implement robust access controls and governance mechanisms around the `upgradeTo` and `upgradeToAndCall` functions. Only trusted entities, such as contract administrators or a multi-signature wallet, should have the authority to invoke these functions.

L19 - Stable Compiler Version

Criticality	Minor / Informative
Location	contracts/token1.sol#L2
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 ^0.8.9;
```

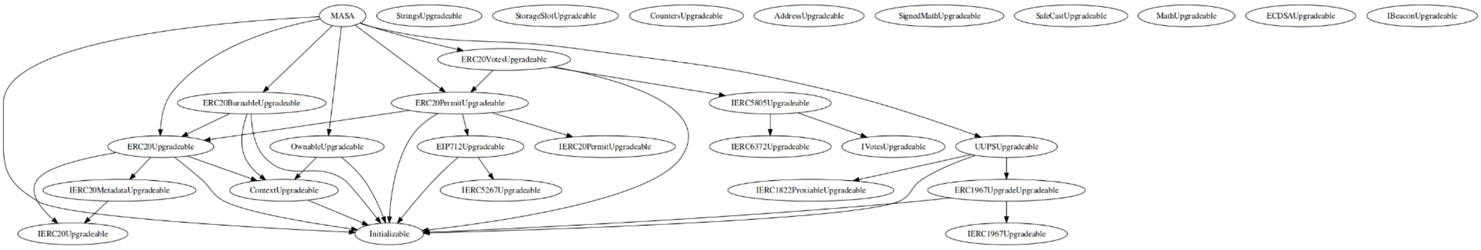
Recommendation

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.

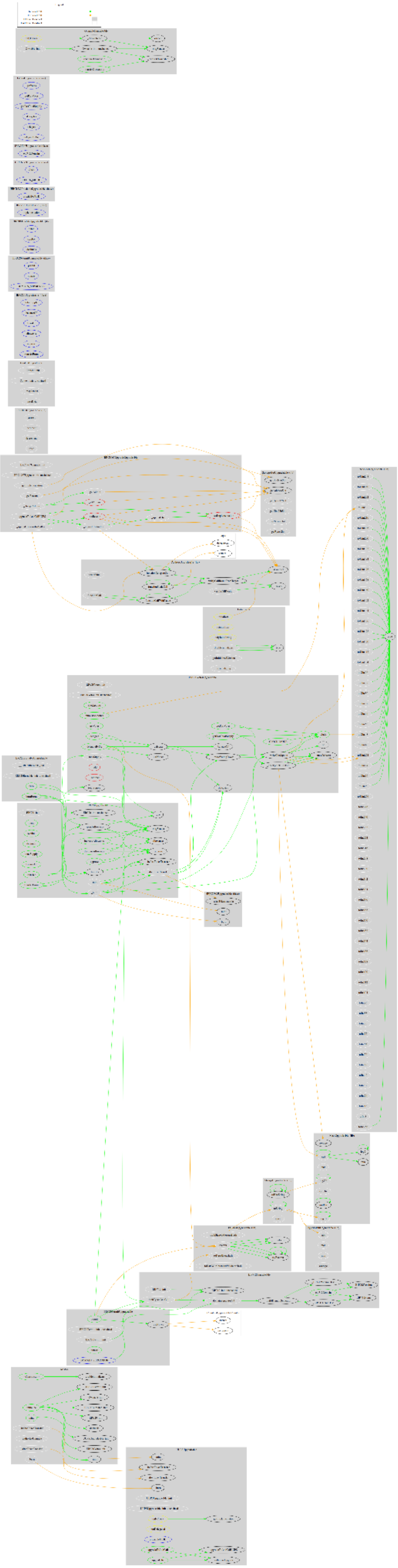
Functions Analysis

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
MASA	Implementation	Initializable, ERC20Upgradeable, ERC20BurnableUpgradeable, OwnableUpgradeable, ERC20PermitUpgradeable, ERC20VotesUpgradeable, UUPSUpgradeable		
		Public	✓	-
	initialize	Public	✓	initializer
	mint	Public	✓	onlyOwner
	_beforeTokenTransfer	Internal	✓	
	_authorizeUpgrade	Internal	✓	onlyOwner
	_afterTokenTransfer	Internal	✓	
	_mint	Internal	✓	
	_burn	Internal	✓	

Inheritance Graph



Flow Graph



Summary

AI MASA contract implements a token mechanism. This audit investigates security issues, business logic concerns and potential improvements. There are some functions that can be abused by the owner like mint tokens. If the contract owner abuses the mint functionality, then the contract will be highly inflated. A multi-wallet signing pattern will provide security against potential hacks. Temporarily locking the contract or renouncing ownership will eliminate all the contract threats.

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