Cyberscope

Audit Report

OctaSpace

July 2024

Network ETH

Address 0x001791385cd8D8b3703AAA2eCc233a2421b8a511

Audited by © cyberscope

Analysis

Critical Medium Minor / Informative Pass

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

Table of Contents

Review

Contract Name	WOCTA
Compiler Version	v0.8.25+commit.b61c2a91
Optimization	9999999 runs
Explorer	https://etherscan.io/address/0x001791385cd8d8b3703aaa2ecc233a2421b8a511
Address	0x001791385cd8d8b3703aaa2ecc233a2421b8a511
Network	ETH
Decimals	18

Audit Updates

Initial Audit	03 Jul 2024

Source Files

Filename	SHA256
WOCTA.sol	1309e9a0b93fc72f5cb54ef7ed516f86ed0b8c3623f36d48067b54bf4ac77e61

Overview

The smart contract audit was conducted for the contract deployed at the implementation address `0x001791385cd8d8b3703aaa2ecc233a2421b8a511`. This contract has been deployed through a proxy contract located at `0xfa704148d516b209d52c2d75f239274c8f8eaf1a`. The implementation address can change, as the proxy contract allows for upgradability, which means the logic of the contract can be modified over time while keeping the same proxy address. This feature is a common practice to enable improvements and updates without disrupting the existing contract interactions.

Findings Breakdown

Critical	0
Medium	2
Minor / Informative	0

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

ST - Stops Transactions

Criticality	Medium
Location	WOCTA.sol#L39
Status	Unresolved

Description

The `PAUSER_ROLE` account has the authority to stop the transactions for all users. The `PAUSER_ROLE` account may take advantage of it by calling the `pause` function.

```
function pause() public onlyRole(PAUSER_ROLE) {
    _pause();
}
```

Recommendation

The team should carefully manage the private keys of the `PAUSER_ROLE` account's account. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the contract `PAUSER_ROLE` functions.

Temporary Solutions:

These measurements do not decrease the severity of the finding

- Introduce a time-locker mechanism with a reasonable delay.
- Introduce a multi-signature wallet so that many addresses will confirm the action.
- Introduce a governance model where users will vote about the actions.

Permanent Solution:

- Renouncing the ownership, which will eliminate the threats but it is non-reversible.

MT - Mints Tokens

Criticality	Medium
Location	WOCTA.sol#L47
Status	Unresolved

Description

The `MINTER_ROLE` account has the authority to mint tokens. The `MINTER_ROLE` account 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
onlyRole(MINTER_ROLE) {
    _mint(to, amount);
}
```

Recommendation

The team should carefully manage the private keys of the `MINTER_ROLE` account. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the contract `MINTER_ROLE` functions.

Temporary Solutions:

These measurements do not decrease the severity of the finding

- Introduce a time-locker mechanism with a reasonable delay.
- Introduce a multi-signature wallet so that many addresses will confirm the action.
- Introduce a governance model where users will vote about the actions.

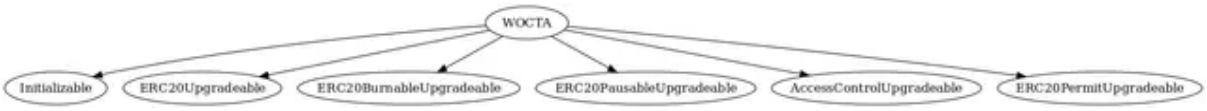
Permanent Solution:

- Renouncing the ownership, which will eliminate the threats but it is non-reversible.

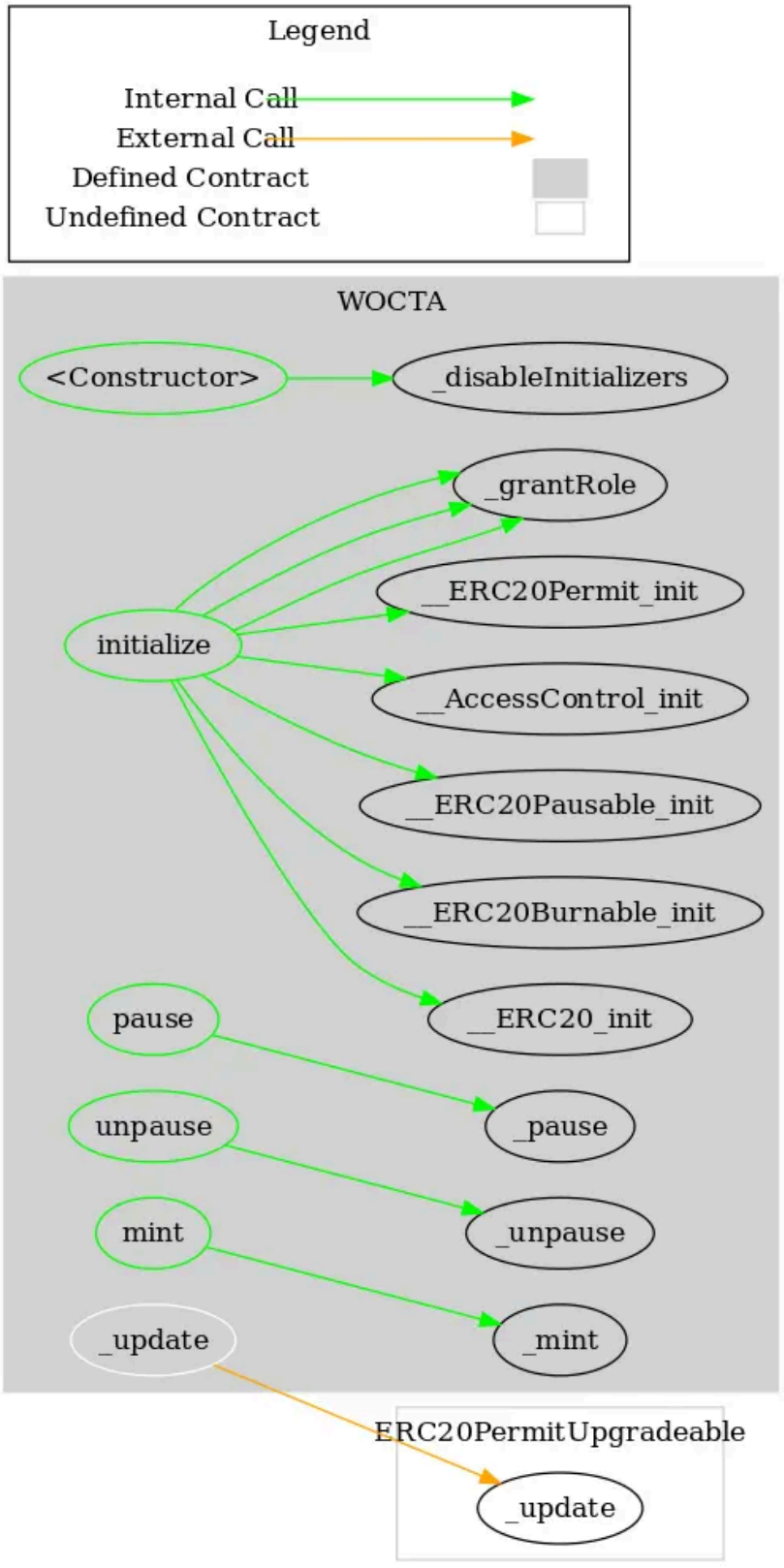
Functions Analysis

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
WOCTA	Implementation	Initializable, ERC20Upgradeable, ERC20BurnableUpgradeable, ERC20PausableUpgradeable, AccessControlUpgradeable, ERC20PermitUpgradeable		
		Public	✓	-
	initialize	Public	✓	initializer
	pause	Public	✓	onlyRole
	unpause	Public	✓	onlyRole
	mint	Public	✓	onlyRole
	_update	Internal	✓	

Inheritance Graph



Flow Graph


Legend
Internal Call
External Call
Defined Contract
Undefined Contract
WOCTA
<Constructor>
_disableInitializers
_grantRole
__ERC20Permit_init
initialize
__AccessControl_init
__ERC20Pausable_init
__ERC20Burnable_init
__ERC20_init
pause
_pause
unpause
_unpause
mint
_mint
_update
ERC20PermitUpgradeable
_update

Summary

OctaSpace 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 certain roles like stop transactions and mint tokens. If 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