Cyberscope

Audit Report

HyDRAULIC

July 2024

Repository	https://github.com/SoloIPmanagement/hydraulic-contracts-audit-internal
Commit	c99464b712db5b8d3fdc3564023b2409609ae682
Audited by	© cyberscope

Table of Contents

Review

Contract Name	DRAU
Repository	https://github.com/SoloIPmanagement/hydraulic-contracts-audit-internal
Commit	c99464b712db5b8d3fdc3564023b2409609ae682
Testing Deploy	https://testnet.bscscan.com/address/0x74f3bfc68d06cc2609d94d891f7a3314a0ceb1ba
Decimals	18

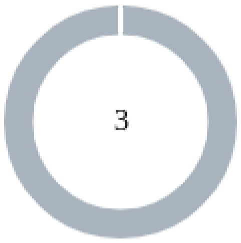
Audit Updates

Initial Audit	12 Jun 2024
Corrected Phase 2	02 Jul 2024

Source Files

Filename	SHA256
contracts/DRAU.sol	430b78f69ddf5368b87a9fd633f7c8776f4a03ad08038b8f666c588682bdfa42

Findings Breakdown



●	Critical	0
●	Medium	0
●	Minor / Informative	3

Severity		Unresolved	Acknowledged	Resolved	Other
●	Critical	0	0	0	0
●	Medium	0	0	0	0
●	Minor / Informative	0	3	0	0

Diagnostics

● Critical ● Medium ● Minor / Informative

Severity	Code	Description	Status
●	MT	Mints Tokens	Acknowledged
●	ST	Stops Transactions	Acknowledged
●	L04	Conformance to Solidity Naming Conventions	Acknowledged

MT - Mints Tokens

Criticality	Minor / Informative
Location	DRAU.sol#L35
Status	Acknowledged

Description

The contract owner has the authority to mint tokens until the `MAXIMUM_SUPPLY` is reached. 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) external onlyOwner
{
        if (totalSupply() + amount > MAXIMUM_SUPPLY) {
            revert MaximumSupplyExceeded();
        }
        _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.

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.
- Minth the `MAXIMUM_SUPPLY` amount of tokens.

ST - Stops Transactions

Criticality	Minor / Informative
Location	contracts/DRAU.sol#L56,67,74
Status	Acknowledged

Description

The contract owner has the authority to stop the transactions for all users including the owner. The owner may pass all transactions by calling the `pause` method. As a result, the transactions of all the users will fail, disrupting normal usage and potentially causing significant inconvenience or financial loss.

```
   function transfer(address to, uint256 amount) public
override whenNotPaused returns (bool) {
        return super.transfer(to, amount);
    }

    function transferFrom(address from, address to, uint256
amount) public override whenNotPaused returns (bool) {
        return super.transferFrom(from, to, amount);
    }

    function pause() external onlyOwner {
        _pause();
    }
```

Recommendation

It is recommended to implement stricter controls and oversight mechanisms around the `pause` function to prevent potential misuse. Additionally, 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.

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.

L04 - Conformance to Solidity Naming Conventions

Criticality	Minor / Informative
Location	contracts/DRAU.sol#L13
Status	Acknowledged

Description

The Solidity style guide is a set of guidelines for writing clean and consistent Solidity code. Adhering to a style guide can help improve the readability and maintainability of the Solidity code, making it easier for others to understand and work with.

The followings are a few key points from the Solidity style guide:

1. Use camelCase for function and variable names, with the first letter in lowercase (e.g., myVariable, updateCounter).
2. Use PascalCase for contract, struct, and enum names, with the first letter in uppercase (e.g., MyContract, UserStruct, ErrorEnum).
3. Use uppercase for constant variables and enums (e.g., MAX_VALUE, ERROR_CODE).
4. Use indentation to improve readability and structure.
5. Use spaces between operators and after commas.
6. Use comments to explain the purpose and behavior of the code.
7. Keep lines short (around 120 characters) to improve readability.

```
uint256 public MAXIMUM_SUPPLY
```

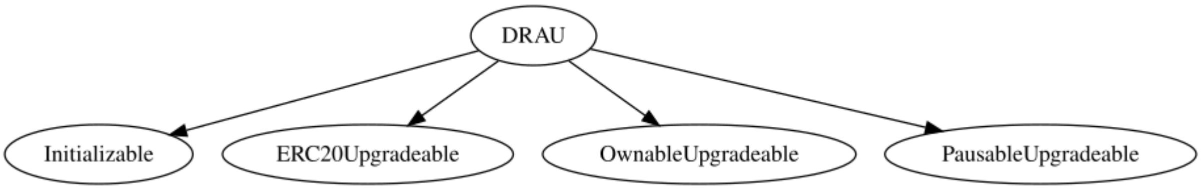
Recommendation

By following the Solidity naming convention guidelines, the codebase increased the readability, maintainability, and makes it easier to work with.
Find more information on the Solidity documentation
https://docs.soliditylang.org/en/v0.8.17/style-guide.html#naming-convention.

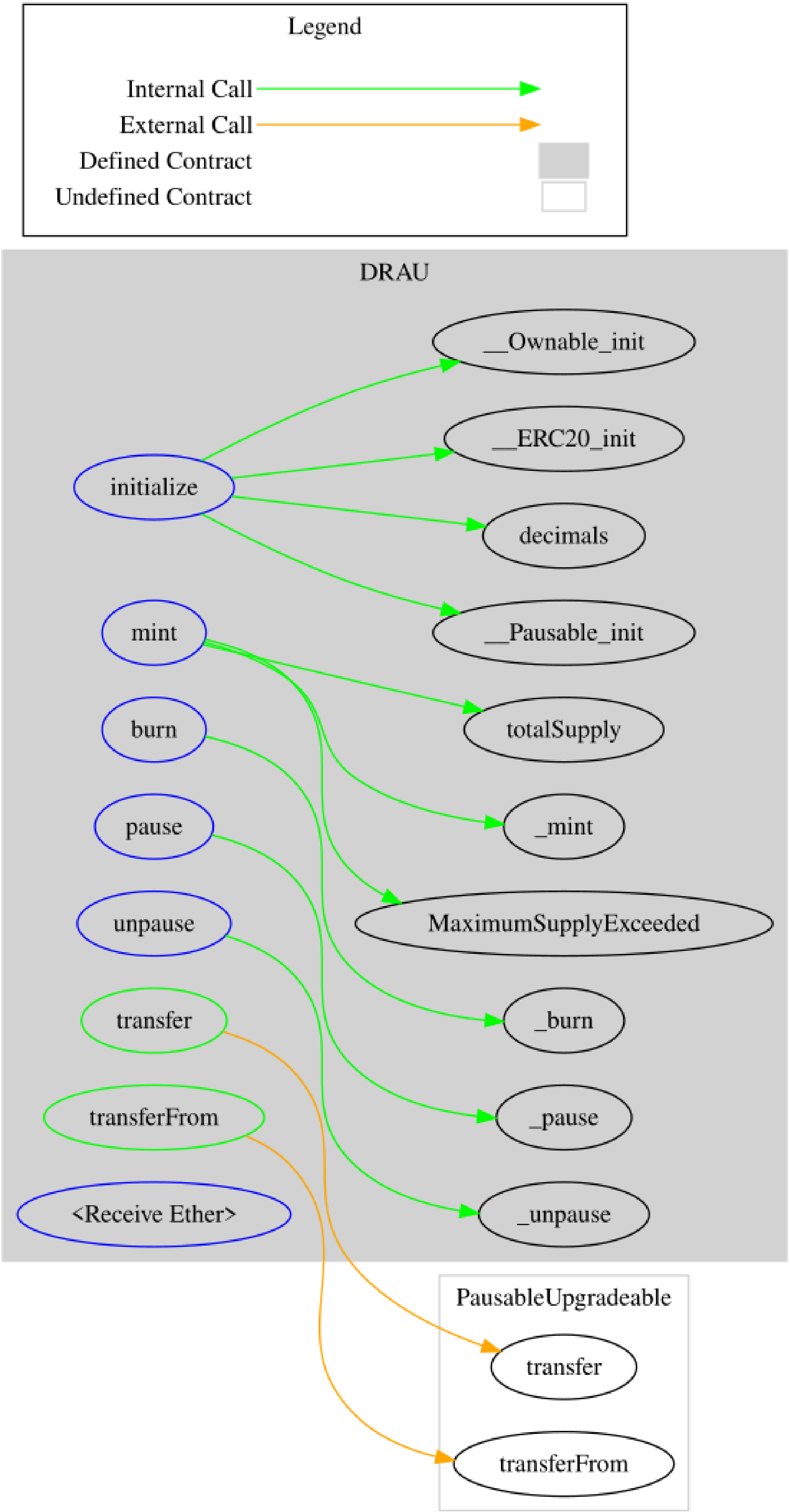
Functions Analysis

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
DRAU	Implementation	Initializable, ERC20Upgradeable, OwnableUpgradeable, PausableUpgradeable		
	initialize	External	✓	initializer
	mint	External	✓	onlyOwner
	burn	External	✓	onlyOwner
	transfer	Public	✓	whenNotPaused
	transferFrom	Public	✓	whenNotPaused
	pause	External	✓	onlyOwner
	unpause	External	✓	onlyOwner
		External	Payable	-

Inheritance Graph



Flow Graph


Legend
Internal Call
External Call
Defined Contract
Undefined Contract
DRAU
__Ownable_init
__ERC20_init
initialize
decimals
__Pausable_init
mint
totalSupply
burn
_mint
pause
MaximumSupplyExceeded
unpause
_burn
transfer
transferFrom
_pause
<Receive Ether>
_unpause
PausableUpgradeable
transfer
transferFrom

Summary

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

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