Cyberscope

Audit Report

UPITFUTURE

January 2025

Network BSC

Address 0x4db7B2FD0A370170a874926B6fd98d34d3D488B5

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
●	MC	Misleading Comments	Unresolved
●	MLI	Missing License Identifier	Unresolved
●	ROF	Redundant Ownable Functionality	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	Universal_Token
Compiler Version	v0.8.16+commit.07a7930e
Optimization	200 runs
Explorer	https://bscscan.com/address/0x4db7b2fd0a370170a874926b6fd98d34d3d488b5
Address	0x4db7b2fd0a370170a874926b6fd98d34d3d488b5
Network	BSC
Symbol	UPiT
Decimals	18
Total Supply	25.000.000

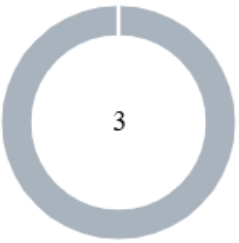
Audit Updates

Initial Audit	22 Jan 2025

Source Files

Filename	SHA256
Universal_Token.sol	6e619c975c8a9438825e018519db95d9a0cdaf7992a64a7df1cff2b8ff0e0429

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	3	0	0	0

MC - Misleading Comments

Criticality	Minor / Informative
Location	Universal_Token.sol#L505,520
Status	Unresolved

Description

The comments are inconsistent. The BEP20Burnable description states that it allows token holders to destroy their own tokens "and those that they have an allowance for." However, the implementation does not include a burnFrom function or similar logic to handle burning tokens based on an allowance, making this claim inaccurate. This is also the case in the comments under the burn function.

```
/**
* @dev Extension of {BEP20} that allows token holders to
destroy both their own
* tokens and those that they have an allowance for, in a way
that can be
* recognized off-chain (via event analysis).
*/
/**
* @dev Destroys `amount` tokens from `account`, deducting from
the caller's allowance.
* See {ERC20-_burn} and {ERC20-allowance}.
* Requirements:
* - the caller must have allowance for ``accounts``'s tokens of
at least `amount`.
*/
```

Recommendation

The team is advised to only add comments that accurately reflect the functionality implemented in the contract. Specifically, the comments should not describe features, such as burning tokens based on an allowance, unless those features are explicitly implemented. Additionally, references to standards (e.g., ERC20 or BEP20) should be consistent and precise throughout the contract to avoid confusion.

MLI - Missing License Identifier

Criticality	Minor / Informative
Location	Universal_Token.sol
Status	Unresolved

Description

The audited smart contract is missing an explicit SPDX license identifier, which is a crucial component for ensuring the legal clarity and compliance of the code. The license identifier specifies the terms under which the code can be used, modified, and redistributed, providing essential guidance to developers and end-users. Its absence creates ambiguity regarding the rights and obligations associated with the code, potentially leading to legal disputes or misuse.

Recommendation

The team is recommended to add an SPDX license identifier to the top of the smart contract to clearly specify the terms under which the code can be used, modified, and distributed.

ROF - Redundant Ownable Functionality

Criticality	Minor / Informative
Location	Universal_Token.sol#L537
Status	Unresolved

Description

The contract inherits from the `Ownable` abstract contract to define an owner. In smart contracts, an owner typically has elevated privileges to execute administrative functions. However, in this case, while the contract defines an owner, it does not include any administrative functionalities other than its own. Therefore, the inheritance of `Ownable` is redundant.

```
contract  Universal_Token is BEP20,Ownable,BEP20Burnable
{/*...*/}
```

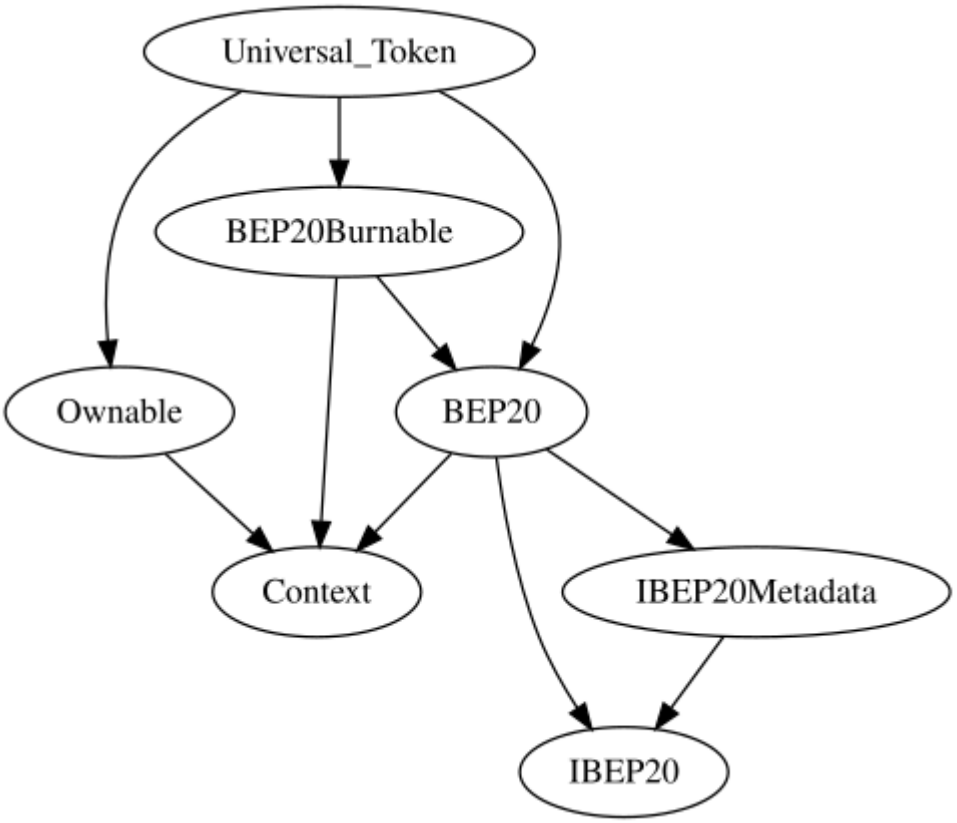
Recommendation

Eliminating redundancies will reduce code size and enhance readability. By removing the unnecessary inheritance, the contract becomes more efficient and aids in future maintainability.

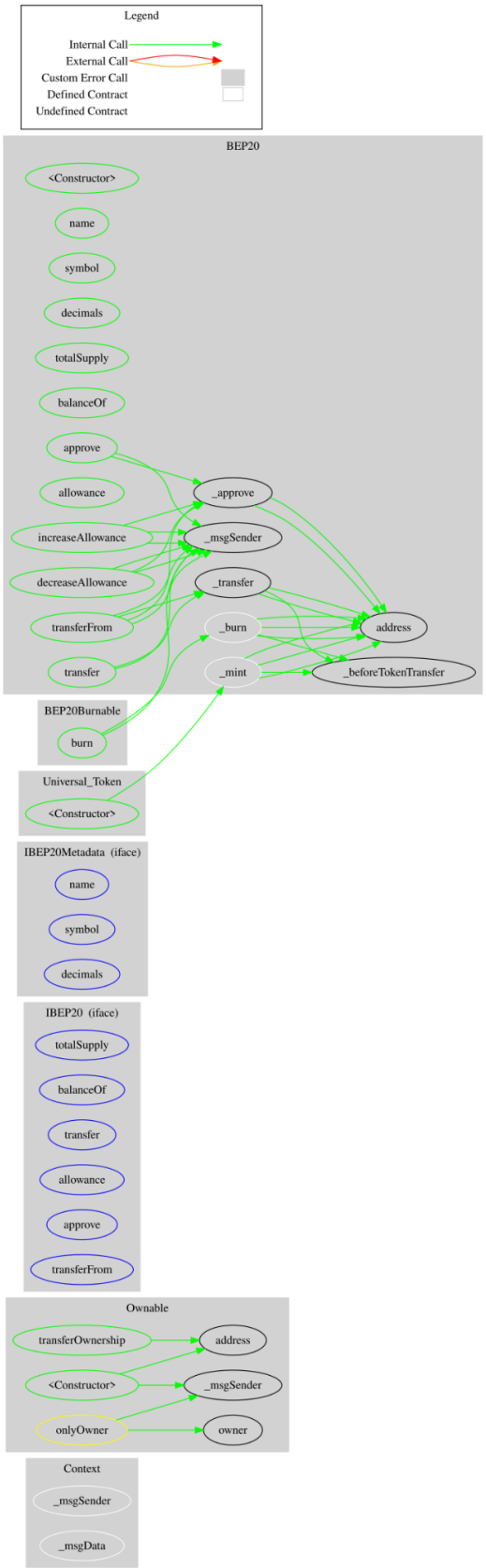
Functions Analysis

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
Universal_Token	Implementation	BEP20, Ownable, BEP20Burnable		
		Public	✓	BEP20

Inheritance Graph



Flow Graph


Legend
Internal Call
External Call
Custom Error Call
Defined Contract
Undefined Contract
BEP20
<Constructor>
name
symbol
decimals
totalSupply
balanceOf
approve
allowance
increaseAllowance
decreaseAllowance
transferFrom
transfer
_approve
_msgSender
_transfer
_burn
_mint
address
_beforeTokenTransfer
BEP20Burnable
burn
Universal_Token
<Constructor>
IBEP20Metadata (iface)
name
symbol
decimals
IBEP20 (iface)
totalSupply
balanceOf
transfer
allowance
approve
transferFrom
Ownable
transferOwnership
address
<Constructor>
_msgSender
onlyOwner
owner
Context
_msgSender
_msgData

Summary

UPITFUTURE contract implements a token mechanism. This audit investigates security issues, business logic concerns and potential improvements. UPITFUTURE is an interesting project that has a friendly and growing community. The Smart Contract analysis reported no critical issues or compiling concerns. The contract owner can access some admin functions that can not be used in a malicious way to disturb the users' transactions. The contract does not implement any fees.

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

cyberscope.io