Cyberscope

Audit Report

Blackjack.fun

March 2024

Network	ETH
Address	0x971b56FD82270bDB578FE68a5805ED424BdD0787
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	Passed
●	BT	Burns Tokens	Passed
●	BC	Blacklists Addresses	Passed

Diagnostics

Critical Medium Minor / Informative

Severity	Code	Description	Status
	L19	Stable Compiler Version	Unresolved

Table of Contents

Review

Contract Name	BlackjackFun
Compiler Version	v0.8.22+commit.4fc1097e
Optimization	200 runs
Explorer	https://etherscan.io/address/0x971b56fd82270bdb578fe68a5805ed424bdd0787
Address	0x971b56fd82270bdb578fe68a5805ed424bdd0787
Network	ETH
Symbol	JACK
Decimals	18
Total Supply	5,000,000,000
Badge Eligibility	Must Fix Criticals

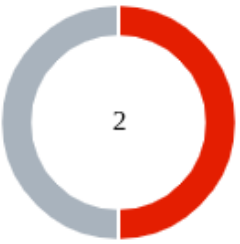
Audit Updates

Initial Audit	21 Mar 2024

Source Files

Filename	SHA256
contract-7414f66777.sol	f14749e278c10ffaa8db06ddbea56a330330d6385d028e969977cb2016919319

Findings Breakdown



Critical	1
Medium	0
Minor / Informative	1

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

ST - Stops Transactions

Criticality	Critical
Location	contract-7414f66777.sol#L24
Status	Unresolved

Description

The `PAUSER_ROLE` address has the authority to stop the transaction for all users including the owner. The `PAUSER_ROLE` may take advantage of it by setting the `pause` to zero. As a result, all the transaction including buys and sells will be prevented.

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

Recommendation

It is recommended that the team reevaluate the necessity of the pause functionality. If it is deemed unnecessary, consider its removal to prevent potential misuse. The team should carefully manage the private keys of the PAUSER_ROLE'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.

L19 - Stable Compiler Version

Criticality	Minor / Informative
Location	contract-7414f66777.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 ^0.8.20;
```

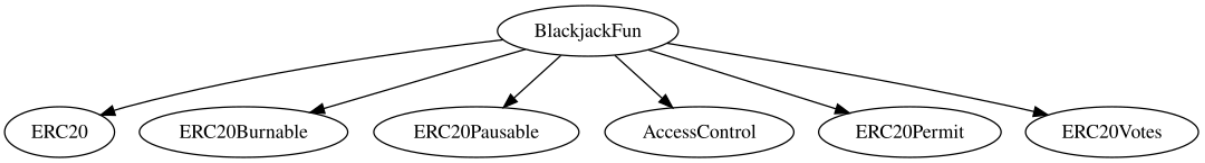
Recommendation

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.

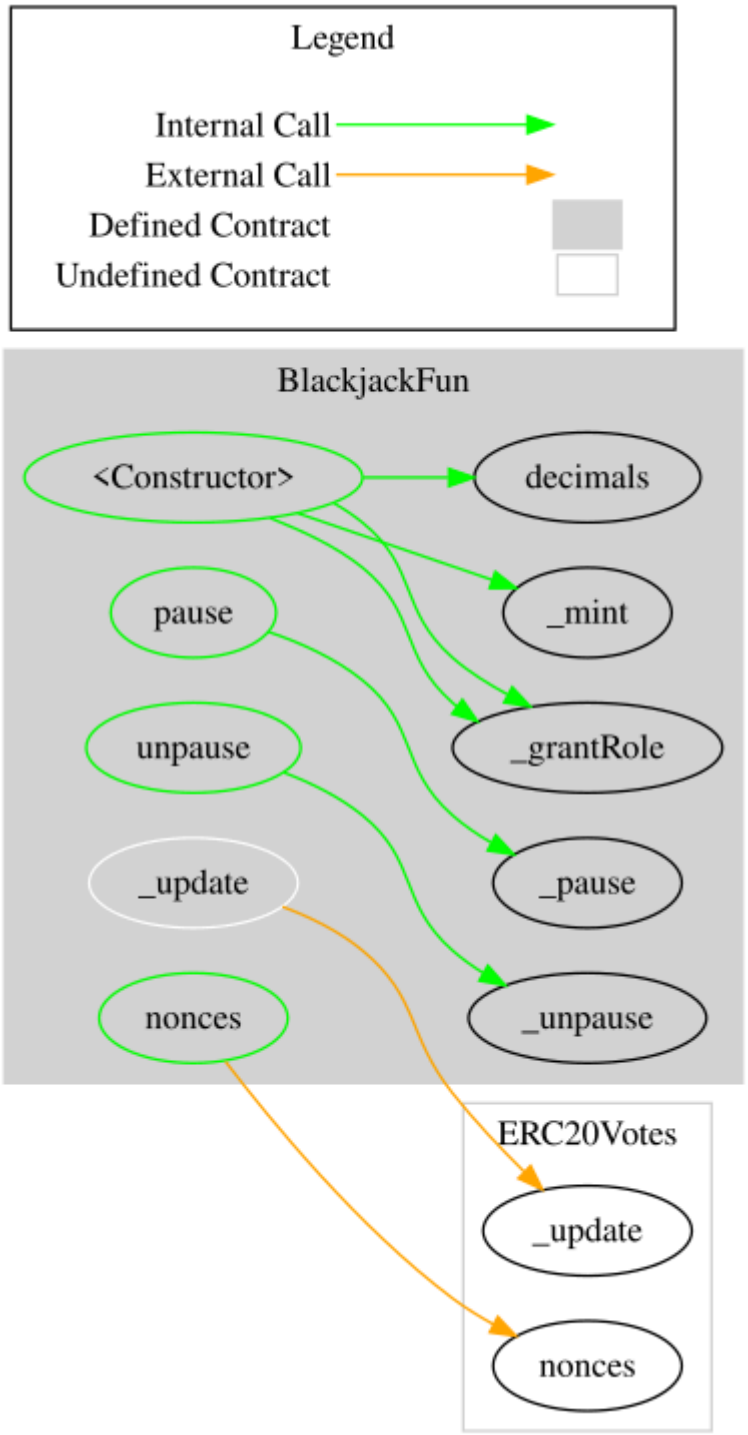
Functions Analysis

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
BlackjackFun	Implementation	ERC20, ERC20Burnable, ERC20Pausable, AccessControl, ERC20Permit, ERC20Votes		
		Public	✓	ERC20 ERC20Permit
	pause	Public	✓	onlyRole
	unpause	Public	✓	onlyRole
	_update	Internal	✓	
	nonces	Public		-

Inheritance Graph



Flow Graph


Legend
Internal Call
External Call
Defined Contract
Undefined Contract
BlackjackFun
<Constructor>
decimals
_mint
pause
_grantRole
unpause
_pause
_update
_unpause
nonces
ERC20Votes
_update
nonces

Summary

Blackjack.fun 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 pauser account like stop transactions. 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