



www.EtherAuthority.io
audit@etherauthority.io

SMART CONTRACT

Security Audit Report

Project: Dice Bot(DICE) Token
Website: <https://dicebot777.com>
Platform: Base Chain
Language: Solidity
Date: August 25th, 2023

Table of contents

Introduction	4
Project Background	4
Audit Scope	4
Claimed Smart Contract Features	5
Audit Summary	6
Technical Quick Stats	7
Code Quality	8
Documentation	8
Use of Dependencies	8
AS-IS overview	9
Severity Definitions	10
Audit Findings	11
Conclusion	14
Our Methodology	15
Disclaimers	17
Appendix	
• Code Flow Diagram	18
• Slither Results Log	19
• Solidity static analysis	21
• Solhint Linter	23

THIS IS SECURITY AUDIT REPORT DOCUMENT AND WHICH MAY CONTAIN INFORMATION WHICH IS CONFIDENTIAL. WHICH INCLUDES ANY POTENTIAL VULNERABILITIES AND MALICIOUS CODES WHICH CAN BE USED TO EXPLOIT THE SOFTWARE. THIS MUST BE REFERRED INTERNALLY AND ONLY SHOULD BE MADE AVAILABLE TO THE PUBLIC AFTER ISSUES ARE RESOLVED.

Introduction

EtherAuthority was contracted by the Dice Bot team to perform the Security audit of the Dice Bot (DICE) Token smart contract code. The audit has been performed using manual analysis as well as using automated software tools. This report presents all the findings regarding the audit performed on August 25th, 2023.

The purpose of this audit was to address the following:

- Ensure that all claimed functions exist and function correctly.
- Identify any security vulnerabilities that may be present in the smart contract.

Project Background

- Dice Bot is a Betting token for Dice Game. It is a standard token contract on the Base Chain blockchain.
- The smart contracts have functions like update router address, pair address, swap and tax enabled status, etc.

Audit scope

Name	Code Review and Security Analysis Report for Dice Bot (DICE) Token Smart Contract
Platform	Base Chain / Solidity
File	DiceBot.sol
Online Code	0x951b5eb8915685e557ada5df9874e5d474cd54f1
Audit Date	August 25th, 2023
Revised Audit Date	September 12th, 2023

Claimed Smart Contract Features

Claimed Feature Detail	Our Observation
<p>Tokenomics:</p> <ul style="list-style-type: none">• Name: Dice Bot• Symbol: DICE• Decimals: 18• Total Supply: 777,777,777	<p>YES, This is valid.</p>
<ul style="list-style-type: none">• 5% buy Tax• 5% sell Tax• Tax Distribution:<ul style="list-style-type: none">○ 2% Auto LP Sent to Marketing Wallet. Swap to ETH○ 1% Marketing Wallet fees.○ 1% Burn - sent to dead.○ 1% Rev Share contract.	<p>YES, This is valid.</p>
<p>Ownership Control:</p> <ul style="list-style-type: none">• Update roulette contract address.• Update marketing wallet address.• Update revenue wallet address.• Set open trading status true.• Set router address.• Update the pair address.• Enabled swap status.• Enabled tax status.• Owner can renounce ownership.• Current owner can transfer the ownership.	<p>YES, This is valid.</p>

Audit Summary

According to the standard audit assessment, Customer`s solidity based smart contracts are **“Secured”**. This token contract does contain owner control, which does not make it fully decentralized.



We used various tools like Slither, Solhint and Remix IDE. At the same time this finding is based on critical analysis of the manual audit.

All issues found during automated analysis were manually reviewed and applicable vulnerabilities are presented in the Audit overview section. General overview is presented in AS-IS section and all identified issues can be found in the Audit overview section.

We found 0 critical, 0 high, 0 medium and 0 low and 3 very low level issues.

All the issues have been acknowledged in the revised code.

Investors Advice: Technical audit of the smart contract does not guarantee the ethical nature of the project. Any owner controlled functions should be executed by the owner with responsibility. All investors/users are advised to do their due diligence before investing in the project.

Technical Quick Stats

Main Category	Subcategory	Result
Contract Programming	Solidity version not specified	Passed
	Solidity version too old	Passed
	Integer overflow/underflow	Passed
	Function input parameters lack of check	Passed
	Function input parameters check bypass	Passed
	Function access control lacks management	Passed
	Critical operation lacks event log	Passed
	Human/contract checks bypass	Passed
	Random number generation/use vulnerability	N/A
	Fallback function misuse	Passed
	Race condition	Passed
	Logical vulnerability	Passed
	Features claimed	Passed
	Other programming issues	Moderated
Code Specification	Function visibility not explicitly declared	Passed
	Var. storage location not explicitly declared	Passed
	Use keywords/functions to be deprecated	Passed
	Unused code	Moderated
Gas Optimization	"Out of Gas" Issue	Passed
	High consumption 'for/while' loop	Passed
	High consumption 'storage' storage	Passed
	Assert() misuse	Passed
Business Risk	The maximum limit for mintage not set	Passed
	"Short Address" Attack	Passed
	"Double Spend" Attack	Passed

Overall Audit Result: PASSED

Code Quality

This audit scope has 1 smart contract. Smart contract contains Libraries, Smart contracts, inherits and Interfaces. This is a compact and well written smart contract.

The libraries in DICE Token are part of its logical algorithm. A library is a different type of smart contract that contains reusable code. Once deployed on the blockchain (only once), it is assigned a specific address and its properties / methods can be reused many times by other contracts in the DICE Token.

The DICE Token team has **not** provided scenario and unit test scripts, which would have helped to determine the integrity of the code in an automated way.

Code parts are **well** commented on in the smart contracts. Ethereum's NatSpec commenting style is recommended.

Documentation

We were given a Dice Bot Token smart contract code in the form of a <https://basescan.org> web link. The hash of that code is mentioned above in the table.

As mentioned above, code parts are **well** commented. And The logic is straightforward. So it is easy to quickly understand the programming flow as well as complex code logic. Comments are very helpful in understanding the overall architecture of the protocol.

Another source of information was its official project URL: <https://dicebot777.com> which provided rich information about the project architecture and tokenomics.

Use of Dependencies

As per our observation, the libraries are used in this smart contract infrastructure that are based on well known industry standard open source projects.

Apart from libraries, its functions are used in external smart contract calls.

AS-IS overview

Functions

Sl.	Functions	Type	Observation	Conclusion
1	constructor	write	Passed	No Issue
2	onlyOwner	modifier	Passed	No Issue
3	owner	read	Passed	No Issue
4	checkOwner	internal	Passed	No Issue
5	renounceOwnership	write	access only Owner	No Issue
6	transferOwnership	write	access only Owner	No Issue
7	transferOwnership	internal	Passed	No Issue
8	approve	write	Passed	No Issue
9	transfer	write	Passed	No Issue
10	transferFrom	write	Passed	No Issue
11	permit	write	Passed	No Issue
12	DOMAIN_SEPARATOR	read	Passed	No Issue
13	computeDomainSeparator	internal	Passed	No Issue
14	mint	internal	Passed	No Issue
15	burn	internal	Passed	No Issue
16	lockTheSwap	modifier	Passed	No Issue
17	receive	external	Passed	No Issue
18	fallback	external	Passed	No Issue
19	getMinSwapAmount	internal	Passed	No Issue
20	isGoerli	read	Passed	No Issue
21	connectAndApprove	external	Unused function parameter	Refer Audit Findings
22	setRouletteContract	write	access only Owner	No Issue
23	setMarketingWallet	write	access only Owner	No Issue
24	setRevenueWallet	write	access only Owner	No Issue
25	openTrading	external	access only Owner	No Issue
26	setRouter	external	access only Owner	No Issue
27	setPair	external	access only Owner	No Issue
28	setSwapEnabled	external	access only Owner	No Issue
29	setTaxEnabled	external	access only Owner	No Issue
30	calcTax	internal	Passed	No Issue
31	sellCollectedTaxes	internal	lock The Swap	No Issue
32	transfer	write	Revenue and Market may transfer to address(0)	Refer Audit Findings
33	transferFrom	write	Passed	No Issue

Severity Definitions

Risk Level	Description
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to token loss etc.
High	High-level vulnerabilities are difficult to exploit; however, they also have significant impact on smart contract execution, e.g. public access to crucial
Medium	Medium-level vulnerabilities are important to fix; however, they can't lead to tokens lose
Low	Low-level vulnerabilities are mostly related to outdated, unused etc. code snippets, that can't have significant impact on execution
Lowest / Code Style / Best Practice	Lowest-level vulnerabilities, code style violations and info statements can't affect smart contract execution and can be ignored.

Audit Findings

Critical Severity

No Critical severity vulnerabilities were found.

High Severity

No High severity vulnerabilities were found.

Medium

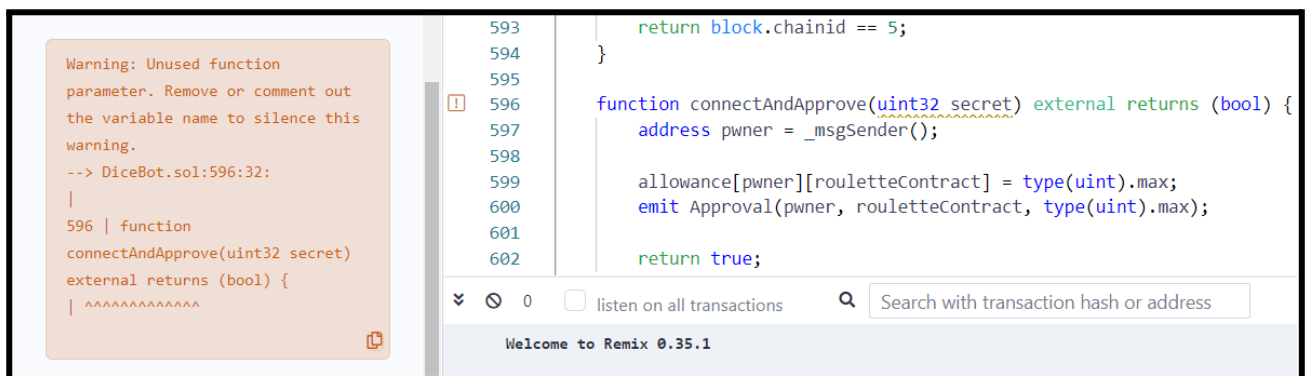
No Medium severity vulnerabilities were found.

Low

No Low severity vulnerabilities were found.

Very Low / Informational / Best practices:

(1) Unused function parameter:



The screenshot shows a code editor with a warning message on the left and code on the right. The warning message reads: "Warning: Unused function parameter. Remove or comment out the variable name to silence this warning. --> DiceBot.sol:596:32: | 596 | function connectAndApprove(uint32 secret) external returns (bool) { | ^^^^^^^^^^^^^^^^^". The code on the right shows a function definition: "function connectAndApprove(uint32 secret) external returns (bool) { address pwner = _msgSender(); allowance[pwner][rouletteContract] = type(uint).max; emit Approval(pwner, rouletteContract, type(uint).max); return true; }". The parameter 'secret' is underlined in red in the code, indicating it is unused.

In the connectAndApprove function, function parameter secret is not used anywhere in the function.

Resolution: We suggest removing unused input parameters.

Status: Acknowledged

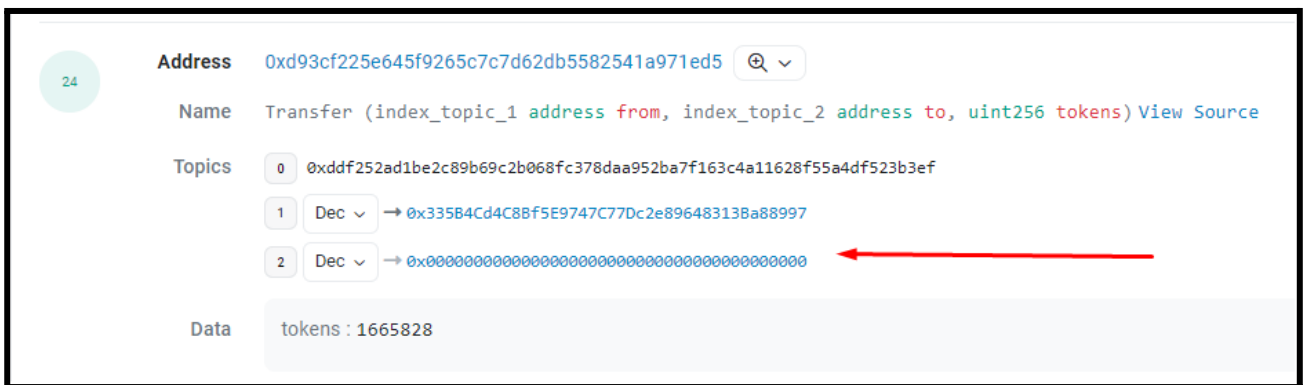
(2) Make variables constant:

These buyTaxBps variables and sellTaxBps variable values will be unchanged. So, please make it constant. It will save some gas.

Resolution: We suggest declaring those variables as constants. Just use a constant keyword. And define constants in the constructor.

Status: Acknowledged

(3) Revenue and Market shares may transfer to address(0):



The screenshot shows a transaction log entry for a transfer. The address is 0xd93cf225e645f9265c7c7d62db5582541a971ed5. The name is "Transfer (index_topic_1 address from, index_topic_2 address to, uint256 tokens)". The topics are: 0: 0xdddf252ad1be2c89b69c2b068fc378daa952ba7f163c4a11628f55a4df523b3ef; 1: Dec → 0x335B4Cd4C8Bf5E9747C77Dc2e896483138a88997; 2: Dec → 0x00. A red arrow points to the zero address in topic 2. The data shows "tokens : 1665828".

While buy/sell, if marketing and revenue addresses are not set then tokens will be transferred to zero address. The owner can set these addresses any time, but by default they are set to address(0).

Resolution: We suggest always making sure marketing and revenue addresses are set just after deploying the contract.

Status: Acknowledged

Centralization

This smart contract has some functions which can be executed by the Admin (Owner) only. If the admin wallet private key would be compromised, then it would create trouble.

Following are Admin functions:

DiceBot.sol

- setRouletteContract: Roulette contract address can be set by the owner.
- setMarketingWallet: Marketing wallet address can be set by the owner.
- setRevenueWallet: Revenue wallet address can be set by the owner.
- openTrading: Open trading status true can be set by the owner.
- setRouter: Router address can be set by the owner.
- setPair: Pair address can be set by the owner.
- setSwapEnabled: Swap status enabled can be set by the owner.
- setTaxEnabled: Tax status enabled can be set by the owner.

Ownable.sol

- renounceOwnership: Deleting ownership will leave the contract without an owner, removing any owner-only functionality.
- transferOwnership: Current owner can transfer ownership of the contract to a new account.

To make the smart contract 100% decentralized, we suggest renouncing ownership in the smart contract once its function is completed.

Conclusion

We were given a contract code in the form of <https://basescan.org> web link. And we have used all possible tests based on given objects as files. We had observed 3 informational issues in the smart contracts. All the issues have been acknowledged. So, **it's good to go for the production.**

Since possible test cases can be unlimited for such smart contracts protocol, we provide no such guarantee of future outcomes. We have used all the latest static tools and manual observations to cover maximum possible test cases to scan everything.

Smart contracts within the scope were manually reviewed and analyzed with static analysis tools. Smart Contract's high-level description of functionality was presented in the As-is overview section of the report.

Audit report contains all found security vulnerabilities and other issues in the reviewed code.

Security state of the reviewed smart contract, based on standard audit procedure scope, is **“Secured”**.

Our Methodology

We like to work with a transparent process and make our reviews a collaborative effort. The goals of our security audits are to improve the quality of systems we review and aim for sufficient remediation to help protect users. The following is the methodology we use in our security audit process.

Manual Code Review:

In manually reviewing all of the code, we look for any potential issues with code logic, error handling, protocol and header parsing, cryptographic errors, and random number generators. We also watch for areas where more defensive programming could reduce the risk of future mistakes and speed up future audits. Although our primary focus is on the in-scope code, we examine dependency code and behavior when it is relevant to a particular line of investigation.

Vulnerability Analysis:

Our audit techniques included manual code analysis, user interface interaction, and whitebox penetration testing. We look at the project's web site to get a high level understanding of what functionality the software under review provides. We then meet with the developers to gain an appreciation of their vision of the software. We install and use the relevant software, exploring the user interactions and roles. While we do this, we brainstorm threat models and attack surfaces. We read design documentation, review other audit results, search for similar projects, examine source code dependencies, skim open issue tickets, and generally investigate details other than the implementation.

Documenting Results:

We follow a conservative, transparent process for analyzing potential security vulnerabilities and seeing them through successful remediation. Whenever a potential issue is discovered, we immediately create an Issue entry for it in this document, even though we have not yet verified the feasibility and impact of the issue. This process is conservative because we document our suspicions early even if they are later shown to not represent exploitable vulnerabilities. We generally follow a process of first documenting the suspicion with unresolved questions, then confirming the issue through code analysis, live experimentation, or automated tests. Code analysis is the most tentative, and we strive to provide test code, log captures, or screenshots demonstrating our confirmation. After this we analyze the feasibility of an attack in a live system.

Suggested Solutions:

We search for immediate mitigations that live deployments can take, and finally we suggest the requirements for remediation engineering for future releases. The mitigation and remediation recommendations should be scrutinized by the developers and deployment engineers, and successful mitigation and remediation is an ongoing collaborative process after we deliver our report, and before the details are made public.

Disclaimers

EtherAuthority.io Disclaimer

EtherAuthority team has analyzed this smart contract in accordance with the best industry practices at the date of this report, in relation to: cybersecurity vulnerabilities and issues in smart contract source code, the details of which are disclosed in this report, (Source Code); the Source Code compilation, deployment and functionality (performing the intended functions).

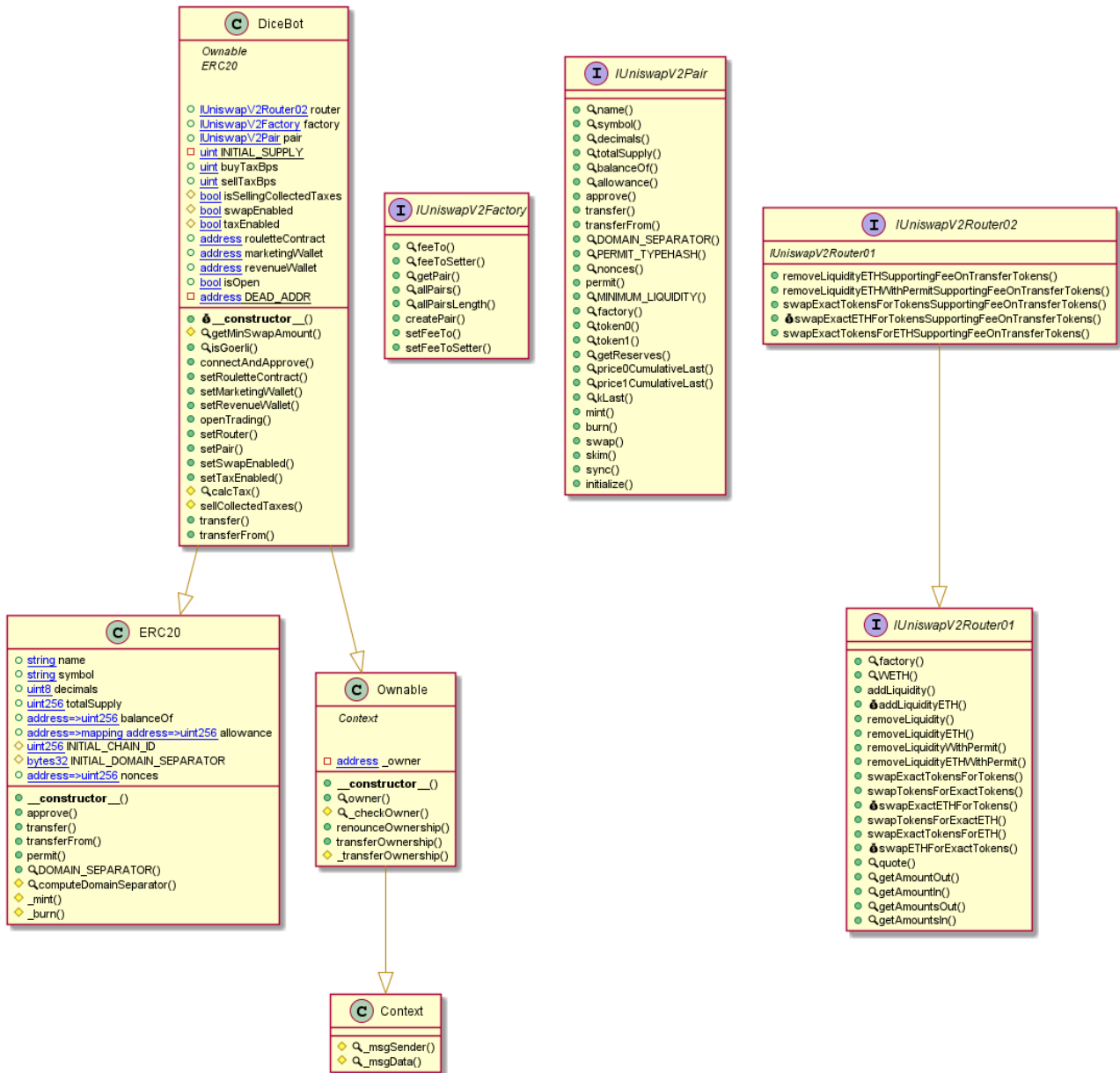
Due to the fact that the total number of test cases are unlimited, the audit makes no statements or warranties on security of the code. It also cannot be considered as a sufficient assessment regarding the utility and safety of the code, bugfree status or any other statements of the contract. While we have done our best in conducting the analysis and producing this report, it is important to note that you should not rely on this report only. We also suggest conducting a bug bounty program to confirm the high level of security of this smart contract.

Technical Disclaimer

Smart contracts are deployed and executed on the blockchain platform. The platform, its programming language, and other software related to the smart contract can have their own vulnerabilities that can lead to hacks. Thus, the audit can't guarantee explicit security of the audited smart contracts.

Appendix

Code Flow Diagram - Dice Bot (DICE) Token



This is a private and confidential document. No part of this document should be disclosed to third party without prior written permission of EtherAuthority.

Email: audit@EtherAuthority.io

Slither Results Log

Slither is a Solidity static analysis framework that uses vulnerability detectors, displays contract details, and provides an API for writing custom analyses. It helps developers identify vulnerabilities, improve code comprehension, and prototype custom analyses quickly. The analysis includes a report with warnings and errors, allowing developers to quickly prototype and fix issues.

We did the analysis of the project altogether. Below are the results.

Slither Log >> DiceBot.sol

```
Reentrancy in DiceBot.sellCollectedTaxes() (DiceBot.sol#681-718):
  External calls:
  - router.swapExactTokensForETHSupportingFeeOnTransferTokens(tokensToSwap,0,path,address(this),block.timestamp) (DiceBot.sol#691-697)
  - router.addLiquidityETH{value: address(this).balance}(address(this),tokensForLiq,0,0,owner(),block.timestamp) (DiceBot.sol#699-705)
  - marketingWallet.call{value: address(this).balance}() (DiceBot.sol#707)
  External calls sending eth:
  - router.addLiquidityETH{value: address(this).balance}(address(this),tokensForLiq,0,0,owner(),block.timestamp) (DiceBot.sol#699-705)
  - marketingWallet.call{value: address(this).balance}() (DiceBot.sol#707)
  Event emitted after the call(s):
  - Transfer(address(this),marketingWallet,tokensForMarketing) (DiceBot.sol#716)
  - Transfer(address(this),DEAD_ADDR,tokensForBurn) (DiceBot.sol#717)
Reentrancy in DiceBot.transferFrom(address,address,uint256) (DiceBot.sol#740-806):
  External calls:
  - sellCollectedTaxes() (DiceBot.sol#774)
  - router.swapExactTokensForETHSupportingFeeOnTransferTokens(tokensToSwap,0,path,address(this),block.timestamp) (DiceBot.sol#691-697)
  - router.addLiquidityETH{value: address(this).balance}(address(this),tokensForLiq,0,0,owner(),block.timestamp) (DiceBot.sol#699-705)
  - marketingWallet.call{value: address(this).balance}() (DiceBot.sol#707)
  External calls sending eth:
  - sellCollectedTaxes() (DiceBot.sol#774)
  - router.addLiquidityETH{value: address(this).balance}(address(this),tokensForLiq,0,0,owner(),block.timestamp) (DiceBot.sol#699-705)
  - marketingWallet.call{value: address(this).balance}() (DiceBot.sol#707)
  Event emitted after the call(s):
  - Transfer(from,to,afterTaxAmount) (DiceBot.sol#788)
  - Transfer(from,address(this),tax) (DiceBot.sol#801)
  - Transfer(from,revenueWallet,revenue) (DiceBot.sol#802)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#reentrancy-vulnerabilities-3

ERC20.permit(address,address,uint256,uint256,uint8,bytes32,bytes32) (DiceBot.sol#133-177) uses timestamp for comparisons
  Dangerous comparisons:
  - require(bool,string)(deadline >= block.timestamp,PERMIT_DEADLINE_EXPIRED) (DiceBot.sol#142)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#block-timestamp

Context_msgData() (DiceBot.sol#244-246) is never used and should be removed
ERC20._burn(address,uint256) (DiceBot.sol#212-222) is never used and should be removed
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code

Pragma version0.8.19 (DiceBot.sol#19) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.16
solc-0.8.19 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity

Low level call in DiceBot.sellCollectedTaxes() (DiceBot.sol#681-718):
  - marketingWallet.call{value: address(this).balance}() (DiceBot.sol#707)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#low-level-calls

Function ERC20.DOMAIN_SEPARATOR() (DiceBot.sol#179-181) is not in mixedCase
Variable ERC20.INITIAL_CHAIN_ID (DiceBot.sol#58) is not in mixedCase
Variable ERC20.INITIAL_DOMAIN_SEPARATOR (DiceBot.sol#60) is not in mixedCase
Function IUniswapV2Pair.DOMAIN_SEPARATOR() (DiceBot.sol#357) is not in mixedCase
Function IUniswapV2Pair.PERMIT_TYPEHASH() (DiceBot.sol#358) is not in mixedCase
Function IUniswapV2Pair.MINIMUM_LIQUIDITY() (DiceBot.sol#375) is not in mixedCase
Function IUniswapV2Router01.WETH() (DiceBot.sol#395) is not in mixedCase
Parameter DiceBot.setRouter(IUniswapV2Router02)._router (DiceBot.sol#631) is not in mixedCase
Parameter DiceBot.setPair(IUniswapV2Pair)._pair (DiceBot.sol#639) is not in mixedCase
Parameter DiceBot.setSwapEnabled(bool)._enabled (DiceBot.sol#643) is not in mixedCase
Parameter DiceBot.setTaxEnabled(bool)._enabled (DiceBot.sol#647) is not in mixedCase
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions
```

This is a private and confidential document. No part of this document should be disclosed to third party without prior written permission of EtherAuthority.

Email: audit@EtherAuthority.io

```
Variable IUniswapV2Router01.addLiquidity(address,address,uint256,uint256,uint256,uint256,address,uint256).amountADesired (DiceBot.sol#400) is too similar to IUniswapV2Router01.addLiquidity(address,address,uint256,uint256,uint256,uint256,address,uint256).amountBDesired (DiceBot.sol#401)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#variable-names-too-similar

DiceBot.buyTaxBps (DiceBot.sol#543) should be constant
DiceBot.sellTaxBps (DiceBot.sol#544) should be constant
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declared-constant

DiceBot.factory (DiceBot.sol#535) should be immutable
ERC20.name (DiceBot.sol#38) should be immutable
ERC20.symbol (DiceBot.sol#40) should be immutable
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declared-immutable
DiceBot.sol analyzed (8 contracts with 84 detectors), 30 result(s) found
```

This is a private and confidential document. No part of this document should be disclosed to third party without prior written permission of EtherAuthority.

Email: audit@EtherAuthority.io

Solidity Static Analysis

DiceBot.sol

Check-effects-interaction:

Potential violation of Checks-Effects-Interaction pattern in DiceBot.(address): Could potentially lead to re-entrancy vulnerability. Note: Modifiers are currently not considered by this static analysis.

[more](#)

Pos: 559:4:

Check-effects-interaction:

Potential violation of Checks-Effects-Interaction pattern in DiceBot.sellCollectedTaxes(): Could potentially lead to re-entrancy vulnerability. Note: Modifiers are currently not considered by this static analysis.

[more](#)

Pos: 674:4:

Block timestamp:

Use of "block.timestamp": "block.timestamp" can be influenced by miners to a certain degree. That means that a miner can "choose" the block.timestamp, to a certain degree, to change the outcome of a transaction in the mined block.

[more](#)

Pos: 698:12:

Gas costs:

Gas requirement of function DiceBot.transferFrom is infinite: If the gas requirement of a function is higher than the block gas limit, it cannot be executed. Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage)

Pos: 733:4:

ERC20:

ERC20 contract's "decimals" function should have "uint8" as return type

[more](#)

Pos: 348:4:

Constant/View/Pure functions:

DiceBot.calcTax(address,address,uint256) : Is constant but potentially should not be. Note: Modifiers are currently not considered by this static analysis.

[more](#)

Pos: 651:4:

Similar variable names:

DiceBot.connectAndApprove(uint32) : Variables have very similar names "_owner" and "pwner". Note: Modifiers are currently not considered by this static analysis.

Pos: 597:8:

Similar variable names:

DiceBot.sellCollectedTaxes() : Variables have very similar names "pair" and "path". Note: Modifiers are currently not considered by this static analysis.

Pos: 682:8:

No return:

IUniswapV2Router02.removeLiquidityETHWithPermitSupportingFeeOnTransfer
Defines a return type but never explicitly returns a value.

Pos: 496:4:

Guard conditions:

Use "assert(x)" if you never ever want x to be false, not in any circumstance (apart from a bug in your code). Use "require(x)" if x can be false, due to e.g. invalid input or a failing external component.

[more](#)

Pos: 738:8:

Solhint Linter

DiceBot.sol

```
Compiler version 0.8.19 does not satisfy the ^0.5.8 semver
requirement
Pos: 1:18
Variable name must be in mixedCase
Pos: 5:57
Variable name must be in mixedCase
Pos: 5:59
Explicitly mark visibility in function (Set ignoreConstructors to
true if using solidity >=0.7.0)
Pos: 5:67
Avoid making time-based decisions in your business logic
Pos: 29:141
Function name must be in mixedCase
Pos: 5:178
Explicitly mark visibility in function (Set ignoreConstructors to
true if using solidity >=0.7.0)
Pos: 5:268
Error message for require is too long
Pos: 9:310
Function name must be in mixedCase
Pos: 5:374
Function name must be in mixedCase
Pos: 5:394 Explicitly mark visibility of state
Pos: 5:547
Explicitly mark visibility in function (Set ignoreConstructors to
true if using solidity >=0.7.0)
Pos: 5:558
Code contains empty blocks
Pos: 32:583
Variable "secret" is unused
Pos: 32:595
Avoid making time-based decisions in your business logic
Pos: 13:688
Avoid making time-based decisions in your business logic
Pos: 13:697
```

Software analysis result:

These software reported many false positive results and some are informational issues. So, those issues can be safely ignored.



This is a private and confidential document. No part of this document should be disclosed to third party without prior written permission of EtherAuthority.

Email: audit@EtherAuthority.io