

Security Assessment:
TG.Bet PreSaleV1

January 11, 2024

TG.Bet

- Audit Status: **Fail**
- Audit Edition: **Advance**



Project Overview

Token Summary

Parameter	Result
Address	
Name	TG.Bet
Token Tracker	TG.Bet (TGB)
Decimals	18
Supply	100,000,000
Platform	Ethereum
compiler	v0.8.19+commit.7dd6d404
Contract Name	PresaleV1
Optimization	Yes with 200 runs
LicenseType	MIT
Language	Solidity
Codebase	https://etherscan.io/ token/0xA908E871B3a70ed2331FcE180AAa871e9536133f#code
Payment Tx	Corporate

Main Contract Assessed Contract Name

Name	Contract	Live
TG.Bet		No

TestNet Contract was Not Assessed

Solidity Code Provided

SolidID	File Sha-1	FileName
TGB	5e0b4e80818a78bfb8c7006aab9c12b02cafe3f2	PresaleV1.sol
TGB		
TGB		
TGB		
TGB		
TGB		

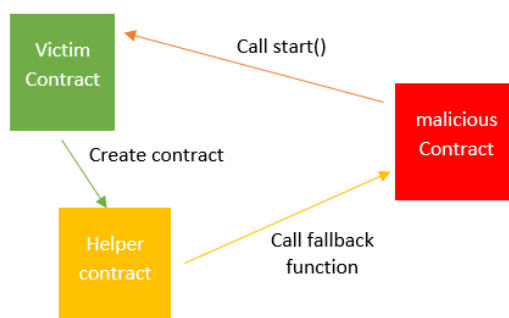
Reentrancy Check

The Project Owners of TG.Bet have not configure the Reentrancy Guard library.

**You can read more about Reentrancy issues in the following link.
[Reentrancy After Istanbul.](#)**

We recommend the team to add the library to the contract to avoid potential issues.

We recommend the team to create a new contract with Reentrancy Guard added to the same.



Smart Contract Vulnerability Checks

The Smart Contract Weakness Classification Registry (SWC Registry) is an implementation of the weakness classification scheme proposed in EIP-1470. It is loosely aligned to the terminologies and structure used in the Common Weakness Enumeration (CWE) while overlaying a wide range of weakness variants that are specific to smart contracts.

ID	Severity	Name	File	location
SWC-100	Pass	Function Default Visibility	PresaleV1.sol	L: 0 C: 0
SWC-101	Pass	Integer Overflow and Underflow.	PresaleV1.sol	L: 0 C: 0
SWC-102	Pass	Outdated Compiler Version file.	PresaleV1.sol	L: 0 C: 0
SWC-103	Pass	A floating pragma is set.	PresaleV1.sol	L: 0 C: 0
SWC-104	Pass	Unchecked Call Return Value.	PresaleV1.sol	L: 0 C: 0
SWC-105	Pass	Unprotected Ether Withdrawal.	PresaleV1.sol	L: 0 C: 0
SWC-106	Pass	Unprotected SELFDESTRUCT Instruction	PresaleV1.sol	L: 0 C: 0
SWC-107	Pass	Read of persistent state following external call.	PresaleV1.sol	L: 0 C: 0
SWC-108	Pass	State variable visibility is not set..	PresaleV1.sol	L: 0 C: 0
SWC-109	Pass	Uninitialized Storage Pointer.	PresaleV1.sol	L: 0 C: 0
SWC-110	Pass	Assert Violation.	PresaleV1.sol	L: 0 C: 0
SWC-111	Pass	Use of Deprecated Solidity Functions.	PresaleV1.sol	L: 0 C: 0
SWC-112	Pass	Delegate Call to Untrusted Callee.	PresaleV1.sol	L: 0 C: 0
SWC-113	Pass	Multiple calls are executed in the same transaction.	PresaleV1.sol	L: 0 C: 0
SWC-114	Pass	Transaction Order Dependence.	PresaleV1.sol	L: 0 C: 0

ID	Severity	Name	File	location
SWC-115	Pass	Authorization through tx.origin.	PresaleV1.sol	L: 0 C: 0
SWC-116	Pass	A control flow decision is made based on The block.timestamp environment variable.	PresaleV1.sol	L: 0 C: 0
SWC-117	Pass	Signature Malleability.	PresaleV1.sol	L: 0 C: 0
SWC-118	Pass	Incorrect Constructor Name.	PresaleV1.sol	L: 0 C: 0
SWC-119	Pass	Shadowing State Variables.	PresaleV1.sol	L: 0 C: 0
SWC-120	Pass	Potential use of block.number as source of randomness.	PresaleV1.sol	L: 0 C: 0
SWC-121	Pass	Missing Protection against Signature Replay Attacks.	PresaleV1.sol	L: 0 C: 0
SWC-122	Pass	Lack of Proper Signature Verification.	PresaleV1.sol	L: 0 C: 0
SWC-123	Pass	Requirement Violation.	PresaleV1.sol	L: 0 C: 0
SWC-124	Pass	Write to Arbitrary Storage Location.	PresaleV1.sol	L: 0 C: 0
SWC-125	Pass	Incorrect Inheritance Order.	PresaleV1.sol	L: 0 C: 0
SWC-126	Pass	Insufficient Gas Griefing.	PresaleV1.sol	L: 0 C: 0
SWC-127	Pass	Arbitrary Jump with Function Type Variable.	PresaleV1.sol	L: 0 C: 0
SWC-128	Pass	DoS With Block Gas Limit.	PresaleV1.sol	L: 0 C: 0
SWC-129	Pass	Typographical Error.	PresaleV1.sol	L: 0 C: 0
SWC-130	Pass	Right-To-Left-Override control character (U+202E).	PresaleV1.sol	L: 0 C: 0
SWC-131	Pass	Presence of unused variables.	PresaleV1.sol	L: 0 C: 0
SWC-132	Pass	Unexpected Ether balance.	PresaleV1.sol	L: 0 C: 0

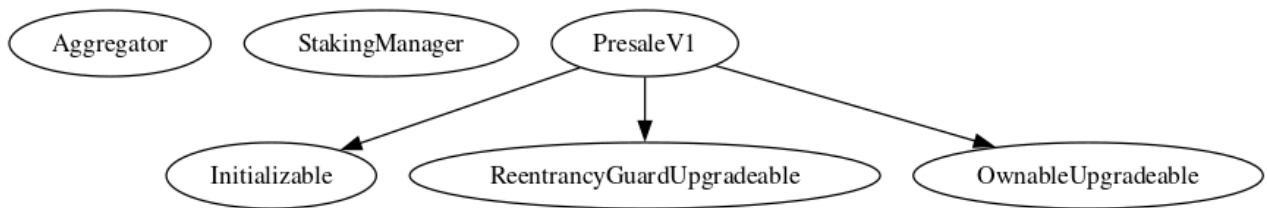
ID	Severity	Name	File	location
SWC-133	Pass	Hash Collisions with Multiple Variable Length Arguments.	PresaleV1.sol	L: 0 C: 0
SWC-134	Pass	Message call with hardcoded gas amount.	PresaleV1.sol	L: 0 C: 0
SWC-135	Pass	Code With No Effects (Irrelevant/Dead Code).	PresaleV1.sol	L: 0 C: 0
SWC-136	Pass	Unencrypted Private Data On-Chain.	PresaleV1.sol	L: 0 C: 0

We scan the contract for additional security issues using MYTHX and industry-standard security scanning tools.

Inheritance

The contract for TG.Bet has the following inheritance structure.

The Project has a Total Supply of 100,000,000





Privileged Functions (onlyOwner)

Please Note if the contract is Renounced none of this functions can be executed.

Function Name	Parameters	Visibility
setTokenPrice		external
setPaymentWallet		external
setMaxTokensToBuy		external
setSaleTimes		external
withdrawRemainingTokens		external

TGB-11 | Unfairness on withdraw - The `withdrawRemainingTokens` function.

Category	Severity	Location	Status
Optimization	 Critical	PresaleV1.sol: L: 479 C: 47	 Detected

Description



Unfairness on withdraw - The `withdrawRemainingTokens` function allows for the owner to withdraw the entire balance of the contract without the presale being over.

Remediation

`withdrawRemainingTokens` should only ever be able to be called after the presale is over.

Project Action

TGB-19 | Potential Logic Issue..

Category	Severity	Location	Status
Optimization	 Critical	PresaleV1.sol: L: 169 C: 47	 Detected

Description



Potential Logic Issue - Transfer Tokens when bought - All `buyWith_` functions transfer tokens to the buyer immediately, however, if this is a presale contract the tokens should not be tradeable and won't be able to be transferred until the token is set to tradeable. Which is a potential unwanted scenario.

Remediation

this function should be revisit.

Project Action

TGB-20 | Potential User Lockout.

Category	Severity	Location	Status
Optimization	 Critical	PresaleV1.sol: L: 490 C: 47	 Detected

Description

Potential User Lockout - Function `setSaleTimes` does not handle all necessary checks for accurate execution.






Remediation

> - Add a check to ensure that the `startTime` is not in the past.- Add a check to ensure that the `endTime` is not in the past.- Add a check to ensure that the `endTime` is not before the `startTime`. ON setting startTime.






Project Action

Technical Findings Summary

Classification of Risk

Severity	Description
 Critical	Risks are those that impact the safe functioning of a platform and must be addressed before launch. Users should not invest in any project with outstanding critical risks.
 High	Risks can include centralization issues and logical errors. Under specific circumstances, these major risks can lead to loss of funds and/or control of the project.
 Medium	Risks may not pose a direct risk to users' funds, but they can affect the overall functioning of a platform
 Low	Risks can be any of the above but on a smaller scale. They generally do not compromise the overall integrity of the Project, but they may be less efficient than other solutions.
 Informational	Errors are often recommended to improve the code's style or certain operations to fall within industry best practices. They usually do not affect the overall functioning of the code.

Findings

Severity	Found	Pending	Resolved
 Critical	3	3	0
 High	0	0	0
 Medium	0	0	0
 Low	0	0	0
 Informational	0	0	0
Total	3	3	0

Social Media Checks

Social Media	URL	Result
Twitter	https://twitter.com/Duchapprovn	Pass
Other	https://medium.com/@Duchapprovn	Pass
Website	https://tg.bet	Pass
Telegram	https://t.me/Duchapprovn	Pass

We recommend to have 3 or more social media sources including a completed working websites.

Social Media Information Notes:

Auditor Notes: undefined

Project Owner Notes:



Assessment Results

Score Results

Review	Score
Overall Score	76/100
Auditor Score	50/100
Review by Section	Score
Manual Scan Score	20
SWC Scan Score	37
Advance Check Score	19

The Following Score System Has been Added to this page to help understand the value of the audit, the maximum score is 100, however to attain that value the project must pass and provide all the data needed for the assessment. Our Passing Score has been changed to 84 Points for a higher standard, if a project does not attain 85% is an automatic failure. Read our notes and final assessment below.

Audit Fail



Assessment Results

Important Notes:

- The following contract has a lot of issues that need to be addressed.
- Adding them to the audit, however, needs to be reviewed.
- supplemental document shared with the team.

Auditor Score =50
Audit Fail



Appendix

Finding Categories

Centralization / Privilege

Centralization / Privilege findings refer to either feature logic or implementation of components that act against the nature of decentralization, such as explicit ownership or specialized access roles in combination with a mechanism to relocate funds.

Gas Optimization

Gas Optimization findings do not affect the functionality of the code but generate different, more optimal EVM opcodes resulting in a reduction on the total gas cost of a transaction.

Logical Issue

Logical Issue findings detail a fault in the logic of the linked code, such as an incorrect notion on how `block.timestamp` works.

Control Flow

Control Flow findings concern the access control imposed on functions, such as owner-only functions being invoke-able by anyone under certain circumstances.

Volatile Code

Volatile Code findings refer to segments of code that behave unexpectedly on certain edge cases that may result in a vulnerability.

Coding Style

Coding Style findings usually do not affect the generated byte-code but rather comment on how to make the codebase more legible and, as a result, easily maintainable.

Inconsistency

Inconsistency findings refer to functions that should seemingly behave similarly yet contain different code, such as a constructor assignment imposing different requirements on the input variables than a setter function.

Coding Best Practices

ERC 20 Coding Standards are a set of rules that each developer should follow to ensure the code meets a set of criteria and is readable by all the developers.

Disclaimer

Assure Defi has conducted an independent security assessment to verify the integrity of and highlight any vulnerabilities or errors, intentional or unintentional, that may be present in the reviewed code for the scope of this assessment. This report does not constitute agreement, acceptance, or advocacy for the Project, and users relying on this report should not consider this as having any merit for financial advice in any shape, form, or nature. The contracts audited do not account for any economic developments that the Project in question may pursue, and the veracity of the findings thus presented in this report relate solely to the proficiency, competence, aptitude, and discretion of our independent auditors, who make no guarantees nor assurance that the contracts are entirely free of exploits, bugs, vulnerabilities or deprecation of technologies.

All information provided in this report does not constitute financial or investment advice, nor should it be used to signal that any persons reading this report should invest their funds without sufficient individual due diligence, regardless of the findings presented. Information is provided 'as is, and Assure Defi is under no covenant to audited completeness, accuracy, or solidity of the contracts. In no event will Assure Defi or its partners, employees, agents, or parties related to the provision of this audit report be liable to any parties for, or lack thereof, decisions or actions with regards to the information provided in this audit report.

The assessment services provided by Assure Defi are subject to dependencies and are under continuing development. You agree that your access 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 with high levels of technical risk and uncertainty. The assessment reports could include false positives, negatives, and unpredictable results. The services may access, and depend upon, multiple layers of third parties.

