



CFG NINJA AUDITS

Security Assessment

Halloween Token

October 20, 2023

Audit Status: Pass

Audit Edition: Pinksale













POWERED BY
BLADE POOL

Risk Analysis

















Classifications of Manual Risk Results

Classification	Description
 Critical	Danger or Potential Problems.
 High	Be Careful or Fail test.
 Low	Pass, Not-Detected or Safe Item.
 Informational	Function Detected

Manual Code Review Risk Results

Contract Privilege	Description
 Buy Tax	0%
 Sale Tax	0%
 Cannot Sale	Pass
 Cannot Sale	Pass
 Max Tax	0%
 Modify Tax	No
 Fee Check	Pass
 Is HoneyPot?	Not Detected
 Trading Cooldown	Not Detected
 Can Pause Trade?	Pass



Contract Priviledge	Description
 Pause Transfer?	Enabled at https://bscscan.com/tx/0x42af763630827a6cd4a67eafab517a1de39a13195def2970a3c992ee2d6e84af
 Max Tx?	Pass
 Is Anti Whale?	Not Detected
 Is Anti Bot?	Not Detected
 Is Blacklist?	Not Detected
 Blacklist Check	Pass
 is Whitelist?	Not Detected
 Can Mint?	Pass
 Is Proxy?	Not Detected
 Can Take Ownership?	Not Detected
 Hidden Owner?	Not Detected
 Owner	0x22431B4532cb1DF51D7348Cc99614909B8e29Ace
 Self Destruct?	Not Detected
 External Call?	Not Detected
 Other?	Not Detected
 Holders	1
 Auditor Confidence	Medium
 KYC Completed	No

The following quick summary it's added to the project overview; however, there are more details about the audit and its results. Please read every detail.



Project Overview

Token Summary

Parameter	Result
Address	0xe2b067FF210b4dA97AA2fA474142e0489F4269c8
Name	Halloween
Token Tracker	Halloween (HALLOWEEN)
Decimals	9
Supply	1,000,000,000
Platform	Binance Smart Chain
compiler	v0.8.17+commit.8df45f5f
Contract Name	HALLOWEEN
Optimization	Yes with 200 runs
LicenseType	MIT
Language	Solidity
Codebase	https://bscscan.com/token/0xe2b067FF210b4dA97AA2fA474142e0489F4269c8#code
Payment Tx	Corporate



Main Contract Assessed Contract Name

Name	Contract	Live
Halloween	0xe2b067FF210b4dA97AA2fA474142e0489F4269c8	Yes

TestNet Contract Assessed Contract Name

Name	Contract	Live
Halloween	0xff85F51563B7399D4D7FCbab5560534B92EFa01B	Yes

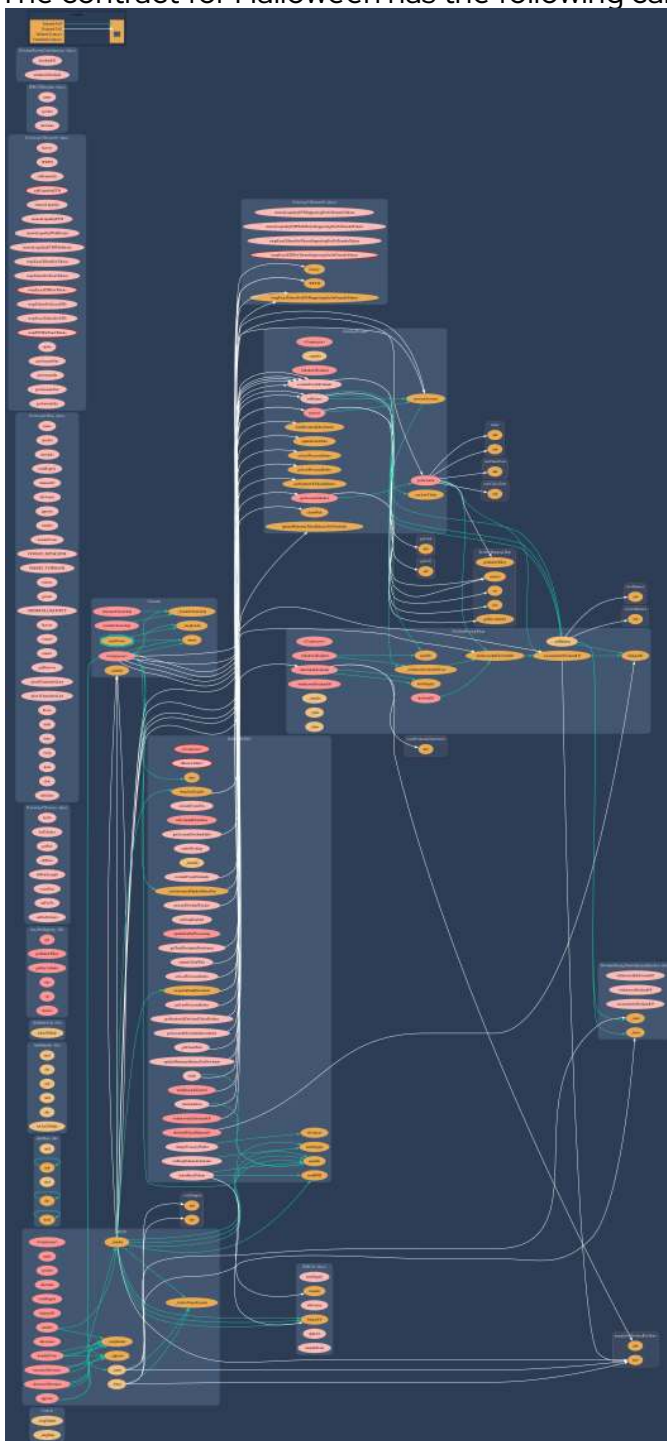
Solidity Code Provided

SolID	File Sha-1	FileName
halloween	c97d3c9783b274e9cbc5d5f8f0f1424e913bb5b7	halloween.sol



Call Graph

The contract for Halloween has the following call graph structure.



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	halloween.sol	L: 0 C: 0
SWC-101	Pass	Integer Overflow and Underflow.	halloween.sol	L: 0 C: 0
SWC-102	Pass	Outdated Compiler Version file.	halloween.sol	L: 0 C: 0
SWC-103	Pass	A floating pragma is set.	halloween.sol	L: 0 C: 0
SWC-104	Pass	Unchecked Call Return Value.	halloween.sol	L: 0 C: 0
SWC-105	Pass	Unprotected Ether Withdrawal.	halloween.sol	L: 0 C: 0
SWC-106	Pass	Unprotected SELFDESTRUCT Instruction	halloween.sol	L: 0 C: 0
SWC-107	Pass	Read of persistent state following external call.	halloween.sol	L: 0 C: 0
SWC-108	Pass	State variable visibility is not set..	halloween.sol	L: 0 C: 0
SWC-109	Pass	Uninitialized Storage Pointer.	halloween.sol	L: 0 C: 0
SWC-110	Pass	Assert Violation.	halloween.sol	L: 0 C: 0



ID	Severity	Name	File	location
SWC-111	Pass	Use of Deprecated Solidity Functions.	halloween.sol	L: 0 C: 0
SWC-112	Pass	Delegate Call to Untrusted Callee.	halloween.sol	L: 0 C: 0
SWC-113	Pass	Multiple calls are executed in the same transaction.	halloween.sol	L: 0 C: 0
SWC-114	Pass	Transaction Order Dependence.	halloween.sol	L: 0 C: 0
SWC-115	Low	Authorization through tx.origin.	halloween.sol	L: 1147 C: 97,L: 1287 C: 90
SWC-116	Pass	A control flow decision is made based on The block.timestamp environment variable.	halloween.sol	L: 0 C: 0
SWC-117	Pass	Signature Malleability.	halloween.sol	L: 0 C: 0
SWC-118	Pass	Incorrect Constructor Name.	halloween.sol	L: 0 C: 0
SWC-119	Pass	Shadowing State Variables.	halloween.sol	L: 0 C: 0
SWC-120	Pass	Potential use of block.number as source of randomness.	halloween.sol	L: 0 C: 0
SWC-121	Pass	Missing Protection against Signature Replay Attacks.	halloween.sol	L: 0 C: 0
SWC-122	Pass	Lack of Proper Signature Verification.	halloween.sol	L: 0 C: 0
SWC-123	Pass	Requirement Violation.	halloween.sol	L: 0 C: 0
SWC-124	Pass	Write to Arbitrary Storage Location.	halloween.sol	L: 0 C: 0



ID	Severity	Name	File	location
SWC-125	Pass	Incorrect Inheritance Order.	halloween.sol	L: 0 C: 0
SWC-126	Pass	Insufficient Gas Griefing.	halloween.sol	L: 0 C: 0
SWC-127	Pass	Arbitrary Jump with Function Type Variable.	halloween.sol	L: 0 C: 0
SWC-128	Pass	DoS With Block Gas Limit.	halloween.sol	L: 0 C: 0
SWC-129	Pass	Typographical Error.	halloween.sol	L: 0 C: 0
SWC-130	Pass	Right-To-Left-Override control character (U+202E).	halloween.sol	L: 0 C: 0
SWC-131	Pass	Presence of unused variables.	halloween.sol	L: 0 C: 0
SWC-132	Pass	Unexpected Ether balance.	halloween.sol	L: 0 C: 0
SWC-133	Pass	Hash Collisions with Multiple Variable Length Arguments.	halloween.sol	L: 0 C: 0
SWC-134	Pass	Message call with hardcoded gas amount.	halloween.sol	L: 0 C: 0
SWC-135	Pass	Code With No Effects (Irrelevant/Dead Code).	halloween.sol	L: 0 C: 0
SWC-136	Pass	Unencrypted Private Data On-Chain.	halloween.sol	L: 0 C: 0

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



Smart Contract Vulnerability Details

SWC-115 - Authorization through tx.origin

CWE-477: Use of Obsolete Function

Description:

tx.origin is a global variable in Solidity which returns the address of the account that sent the transaction. Using the variable for authorization could make a contract vulnerable if an authorized account calls into a malicious contract. A call could be made to the vulnerable contract that passes the authorization check since tx.origin returns the original sender of the transaction which in this case is the authorized account.

Remediation:

tx.origin should not be used for authorization. Use msg.sender instead.

References:

Solidity Documentation - tx.origin

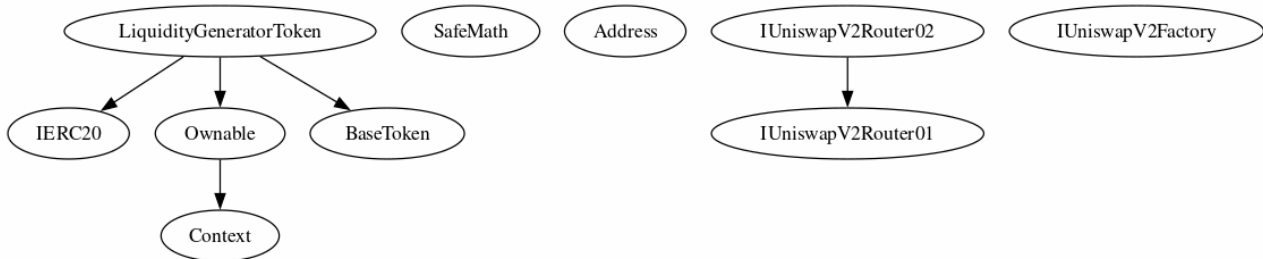
Ethereum Smart Contract Best Practices - Avoid using tx.origin

SigmaPrime - Visibility.



Inheritance

The contract for Halloween has the following inheritance structure.



Smart Contract Advance Checks



ID	Severity	Name	Result	Status
HALLOWEE N-01	Low	Potential Sandwich Attacks.	Pass	Not-Found
HALLOWEE N-02	Informational	Function Visibility Optimization	Fail	Detected
HALLOWEE N-03	Low	Lack of Input Validation.	Fail	Detected
HALLOWEE N-04	High	Centralized Risk In addLiquidity.	Pass	Not-Found
HALLOWEE N-05	Low	Missing Event Emission.	Pass	Detected
HALLOWEE N-06	Low	Conformance with Solidity Naming Conventions.	Pass	Not-Found
HALLOWEE N-07	Low	State Variables could be Declared Constant.	Pass	Not-Found
HALLOWEE N-08	Low	Dead Code Elimination.	Pass	Not-Found
HALLOWEE N-09	High	Third Party Dependencies.	Pass	Detected
HALLOWEE N-10	High	Initial Token Distribution.	Pass	Not-Found
HALLOWEE N-11	High	claimStuckTokens can claim own tokens.	Pass	Detected
HALLOWEE N-12	High	Centralization Risks In The X Role	Pass	Not-Found
HALLOWEE N-13	Informational	Extra Gas Cost For User..	Pass	Detected



ID	Severity	Name	Result	Status
HALLOWEE N-14	Medium	Unnecessary Use Of SafeMath	Fail	Detected
HALLOWEE N-15	Medium	Symbol Length Limitation due to Solidity Naming Standards.	Pass	Detected
HALLOWEE N-16	Medium	Taxes can be up to 100%	Pass	Not Detected
HALLOWEE N-17	Logical Issue	Highly Permissive Role Access.`,`	Pass	Detected
HALLOWEE N-18	Critical	Stop Transactions by using Enable Trade.	Pass	Not Detected



HALLOWEEN-02 | Function Visibility Optimization.

Category	Severity	Location	Status
Gas Optimization	 Informational	halloween.sol: L: 870 C: 14	 Detected

Description

The following functions are declared as public and are not invoked in any of the contracts contained within the projects scope:

Function Name	Parameters	Visibility
renounceOwnership		public
transferOwnership		public
processAccount		public

The functions that are never called internally within the contract should have external visibility

Remediation



We advise that the function's visibility specifiers are set to external, and the array-based arguments change their data location from memory to calldata, optimizing the gas cost of the function.

References:

external vs public best practices.



HALLOWEEN-03 | Lack of Input Validation.

Category	Severity	Location	Status
Volatile Code	 Low	halloween.sol: L: 787 C: 14, L: 289 C: 14	 Detected

Description

The given input is missing the check for the non-zero address.

The given input is missing the check for the setSwapEnabled, .

Remediation



We advise the client to add the check for the passed-in values to prevent unexpected errors as below:

```
...  
require(receiver != address(0), "Receiver is the zero address");  
...  
...  
require(value X limitation, "Your not able to do this function");  
...
```

We also recommend customer to review the following function that is missing a required validation. setSwapEnabled, .



HALLOWEEN-14 | Unnecessary Use Of SafeMath

Category	Severity	Location	Status
Logical Issue	 Medium	halloween.sol: L: 53 C: 0	 Detected

Description

The SafeMath library is used unnecessarily. With Solidity compiler versions 0.8.0 or newer, arithmetic operations will automatically revert in case of integer overflow or underflow.

```
library SafeMath {  
    An implementation of SafeMath library is found.  
    using SafeMath for uint256;  
    SafeMath library is used for uint256 type in contract.
```

Remediation






We advise removing the usage of SafeMath library and using the built-in arithmetic operations provided by the Solidity programming language

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	0	0	0
 High	0	0	0
 Medium	1	0	0
 Low	1	0	0
 Informational	1	0	0
Total	3	0	0



Social Media Checks

Social Media	URL	Result
Twitter	https://twitter.com/HalloweenCryp	Pass
Other		Fail
Website	https://halloweencrypto.fun/	Pass
Telegram	https://t.me/HalloweenCrypto	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	86/100
Auditor Score	85/100
Review by Section	Score
Manual Scan Score	22/33
SWC Scan Score	35 /37
Advance Check Score	29 /30

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 80 Points, if a project does not attain 80% is an automatic failure. Read our notes and final assessment below.

Audit Passed



Assessment Results

Important Notes:

- Project Owner enabled trade and audit is passed.
- Please DYOR on the project.

Auditor Score =85
Audit Passed



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

CFGNINJA 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 CFGNINJA is under no covenant to audited completeness, accuracy, or solidity of the contracts. In no event will CFGNINJA 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 CFGNINJA 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.

