CERTIK

Security Assessment

Safe Energy

Aug 19th, 2021

Table of Contents

Summary

This report has been prepared for Safe Energy to discover issues and vulnerabilities in the source code of the Safe Energy project as well as any contract dependencies that were not part of an officially recognized library. A comprehensive examination has been performed, utilizing Static Analysis and Manual Review techniques.

The auditing process pays special attention to the following considerations:

- Testing the smart contracts against both common and uncommon attack vectors.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

The security assessment resulted in findings that ranged from critical to informational. We recommend addressing these findings to ensure a high level of security standards and industry practices. We suggest recommendations that could better serve the project from the security perspective:

- Enhance general coding practices for better structures of source codes;
- Add enough unit tests to cover the possible use cases;
- Provide more comments per each function for readability, especially contracts that are verified in public;
- Provide more transparency on privileged activities once the protocol is live.

Overview

Project Summary

Project Name	Safe Energy
Platform	BSC
Language	Solidity
Codebase	BSC deplyment address: 0xBBe899c61198D1826a43e20ea19efC46E50c2B00
Commit	

Audit Summary

Delivery Date	Aug 19, 2021
Audit Methodology	Static Analysis, Manual Review
Key Components	

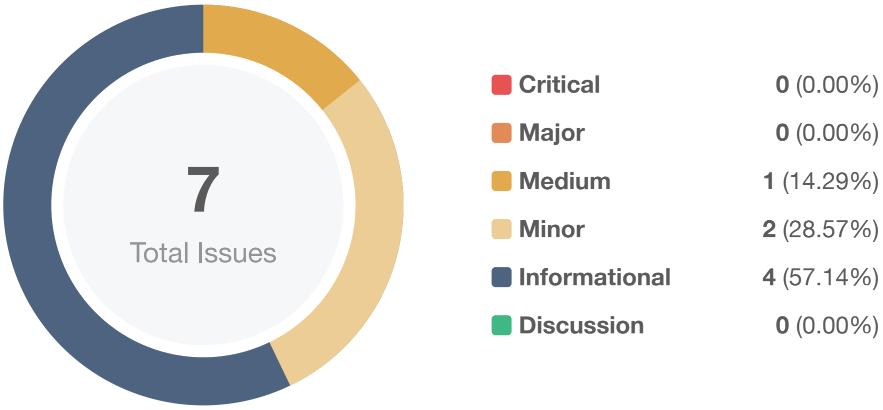
Vulnerability Summary

Vulnerability Level	Total	Pending	Declined	Acknowledged	Partially Resolved	Resolved
Critical	0	0	0	0	0	0
Major	0	0	0	0	0	0
Medium	1	0	0	1	0	0
Minor	2	0	0	2	0	0
Informational	4	0	0	4	0	0
Discussion	0	0	0	0	0	0

Audit Scope

ID	File	SHA256 Checksum
SEC	SafeEnergy.sol	7ca033337978bdc7c60d4d9e800e765c77676854169b47b67a15befe8f79a795

Findings



ID	Title	Category	Severity	Status
SEC-01	Incorrect Error Message	Logical Issue	Minor	Acknowledged
SEC-02	Function Visibility Optimization	Gas Optimization	Informational	Acknowledged
SEC-03	Redundant Code	Logical Issue	Informational	Acknowledged
SEC-04	Incorrect Error Message	Logical Issue	Minor	Acknowledged
SEC-05	Redundant calculation of rBurn	Logical Issue	Informational	Acknowledged
SEC-06	Incorrect address used as Uniswap router	Data Flow	Medium	Acknowledged
SEC-07	Missing Emit Events	Coding Style	Informational	Acknowledged

SEC-01 | Incorrect Error Message

Category	Severity	Location	Status
Logical Issue	Minor	SafeEnergy.sol: 613	Acknowledged

Description

The error message in the require statement in the `includeAccount()` function does not describe the error correctly.

```
function includeAccount(address account) external onlyOwner() {
    require(_isExcluded[account], "Account is already excluded");
```

Recommendation

The message "Account is already excluded" can be changed to "Account is not excluded" .

SEC-02 | Function Visibility Optimization

Category	Severity	Location	Status
Gas Optimization	Informational	SafeEnergy.sol: 479	Acknowledged

Description

The following functions are declared as `public`, and are not invoked in any of the contracts contained within the project's scope. The functions that are never called internally within the contract can be set to external visibility for gas optimization.

- `name()`
- `symbol()`
- `decimals()`
- `totalSupply()`
- `balanceOf(address)`
- `transfer(address,uint256)`
- `allowance(address,address)`
- `approve(address,uint256)`
- `transferFrom(address,address,uint256)`
- `increaseAllowance(address,uint256)`
- `decreaseAllowance(address,uint256)`
- `isExcluded(address)`
- `totalFees()`
- `deliver(uint256)`

Recommendation

We advise that the functions' visibility specifiers are set to `external`, optimizing the gas cost of the function.

SEC-03 | Redundant Code

Category	Severity	Location	Status
Logical Issue	Informational	SafeEnergy.sol: 645~647	Acknowledged

Description

The condition `!_isExcluded[sender] && !_isExcluded[recipient]` can be included in `else` .

Recommendation

The following code can be removed:

```
... else if (!_isExcluded[sender] && !_isExcluded[recipient]) {
    _transferStandard(sender, recipient, amount);
}
```

SEC-04 | Incorrect Error Message

Category	Severity	Location	Status
Logical Issue	Minor	SafeEnergy.sol: 749, 754	Acknowledged

Description

The error message in the `require` statement in function `_setTaxFee()` and `_setBurnFee()` does not describe the error correctly.

```
function _setTaxFee(uint256 taxFee) external onlyOwner() {
    require(taxFee >= 50 && taxFee <= 1000, 'taxFee should be in 1 - 10');
    _TAX_FEE = taxFee;
}

function _setBurnFee(uint256 burnFee) external onlyOwner() {
    require(burnFee >= 50 && burnFee <= 1000, 'burnFee should be in 1 - 10');
    _BURN_FEE = burnFee;
}
```

Recommendation

The message can be changed to 'taxFee/burnFee should be in 0.5 - 10'

SEC-05 | Redundant calculation of rBurn

Category	Severity	Location	Status
Logical Issue	● Informational	SafeEnergy.sol: 655, 657, 665, 667, 676, 678, 687, 689, 722	ⓘ Acknowledged

Description

There are 4 transfer-related functions in the scope: `_transferStandard(), _transferToExcluded(), _transferFromExcluded(), _transferBothExcluded()`. In each of these functions, the value of `rBurn` is calculated, and the function `getRValues()` is called, which calculates `rBurn` again.

Recommendation

Consider adding `rBurn` into the return value in function `_getRValues()` and removing the statements to calculate rBurn in the 4 transfer-related functions. This change should require updates in all other functions that called `_getRValues()`. The following is an example with function `_transferStandard()`

```
function _transferStandard(address sender, address recipient, uint256 tAmount) private {
    //uint256 currentRate =  _getRate();
    (uint256 rAmount, uint256 rTransferAmount, uint256 rFee, uint256 tTransferAmount, uint256 tFee, uint256 tBurn, uint256 rBurn) = _getValues(tAmount);
    //uint256 rBurn =  tBurn.mul(currentRate);
    _rOwned[sender] = _rOwned[sender].sub(rAmount);
    _rOwned[recipient] = _rOwned[recipient].add(rTransferAmount);
    _reflectFee(rFee, rBurn, tFee, tBurn);
    emit Transfer(sender, recipient, tTransferAmount);
}
...
function _getValues(uint256 tAmount) private view returns (uint256, uint256, uint256, uint256, uint256, uint256, uint256) {
    (uint256 tTransferAmount, uint256 tFee, uint256 tBurn) = _getTValues(tAmount, _TAX_FEE, _BURN_FEE);
    uint256 currentRate =  _getRate();
    (uint256 rAmount, uint256 rTransferAmount, uint256 rFee, uint256 rBurn) = _getRValues(tAmount, tFee, tBurn, currentRate);
    return (rAmount, rTransferAmount, rFee, tTransferAmount, tFee, tBurn, rBurn);
}
...
function _getRValues(uint256 tAmount, uint256 tFee, uint256 tBurn, uint256 currentRate) private pure returns (uint256, uint256, uint256, uint256) {
    uint256 rAmount = tAmount.mul(currentRate);
    uint256 rFee = tFee.mul(currentRate);
    uint256 rBurn = tBurn.mul(currentRate);
    uint256 rTransferAmount = rAmount.sub(rFee).sub(rBurn);
```

```
    return (rAmount, rTransferAmount, rFee, rBurn);
}
```

SEC-06 | Incorrect address used as Uniswap router

Category	Severity	Location	Status
Data Flow	Medium	SafeEnergy.sol: 603	Acknowledged

Description

The Uniswap router address used in the require statement is on Ethereum Mainnet instead of BSC (Binance Smart Chain).

```
require(account != 0x7a250d5630B4cF539739dF2C5dAcb4c659F2488D, 'We can not exclude Uniswap router.');
```

Recommendation

If the design specifies that the Uniswap router address should not be the input of function `excludeAccount()`, please use the legit Uniswap router address on BSC.

SEC-07 | Missing Emit Events

Category	Severity	Location	Status
Coding Style	● Informational	SafeEnergy.sol: 748, 753	ⓘ Acknowledged

Description

The function that affects the status of sensitive variables should be able to emit events as notifications to users.

- `setTaxFee()`
- `setBurnFee()`

Recommendation

Consider adding events for sensitive actions, and emit them in the function.

Appendix

Finding Categories

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.

Data Flow

Data Flow findings describe faults in the way data is handled at rest and in memory, such as the result of a struct assignment operation affecting an in-memory struct rather than an in-storage one.

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.

Checksum Calculation Method

The "Checksum" field in the "Audit Scope" section is calculated as the SHA-256 (Secure Hash Algorithm 2 with digest size of 256 bits) digest of the content of each file hosted in the listed source repository under the specified commit.

The result is hexadecimal encoded and is the same as the output of the Linux "sha256sum" command against the target file.

Disclaimer

This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, disclaimer and limitation of liability) set forth in the Services Agreement, or the scope of services, and terms and conditions provided to you (“Customer” or the “Company”) in connection with the Agreement. This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement. 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 CertiK’s prior written consent in each instance.

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 considered, an indication of the economics or value of any “product” or “asset” created by any team or project that contracts CertiK to perform a security assessment. This report 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 in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing 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. CertiK’s position is that each company and individual are responsible for their own due diligence and continuous security. CertiK’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 CertiK is subject to dependencies and 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.

ALL SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF ARE PROVIDED “AS IS” AND “AS

AVAILABLE" AND WITH ALL FAULTS AND DEFECTS WITHOUT WARRANTY OF ANY KIND. TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, CERTIK HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS. WITHOUT LIMITING THE FOREGOING, CERTIK SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM COURSE OF DEALING, USAGE, OR TRADE PRACTICE. WITHOUT LIMITING THE FOREGOING, CERTIK MAKES NO WARRANTY OF ANY KIND THAT THE SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF, WILL MEET CUSTOMER'S OR ANY OTHER PERSON'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULT, BE COMPATIBLE OR WORK WITH ANY SOFTWARE, SYSTEM, OR OTHER SERVICES, OR BE SECURE, ACCURATE, COMPLETE, FREE OF HARMFUL CODE, OR ERROR-FREE. WITHOUT LIMITATION TO THE FOREGOING, CERTIK PROVIDES NO WARRANTY OR UNDERTAKING, AND MAKES NO REPRESENTATION OF ANY KIND THAT THE SERVICE WILL MEET CUSTOMER'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULTS, BE COMPATIBLE OR WORK WITH ANY OTHER SOFTWARE, APPLICATIONS, SYSTEMS OR SERVICES, OPERATE WITHOUT INTERRUPTION, MEET ANY PERFORMANCE OR RELIABILITY STANDARDS OR BE ERROR FREE OR THAT ANY ERRORS OR DEFECTS CAN OR WILL BE CORRECTED.

WITHOUT LIMITING THE FOREGOING, NEITHER CERTIK NOR ANY OF CERTIK'S AGENTS MAKES ANY REPRESENTATION OR WARRANTY OF ANY KIND, EXPRESS OR IMPLIED AS TO THE ACCURACY, RELIABILITY, OR CURRENCY OF ANY INFORMATION OR CONTENT PROVIDED THROUGH THE SERVICE. CERTIK WILL ASSUME NO LIABILITY OR RESPONSIBILITY FOR (I) ANY ERRORS, MISTAKES, OR INACCURACIES OF CONTENT AND MATERIALS OR FOR ANY LOSS OR DAMAGE OF ANY KIND INCURRED AS A RESULT OF THE USE OF ANY CONTENT, OR (II) ANY PERSONAL INJURY OR PROPERTY DAMAGE, OF ANY NATURE WHATSOEVER, RESULTING FROM CUSTOMER'S ACCESS TO OR USE OF THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS.

ALL THIRD-PARTY MATERIALS ARE PROVIDED "AS IS" AND ANY REPRESENTATION OR WARRANTY OF OR CONCERNING ANY THIRD-PARTY MATERIALS IS STRICTLY BETWEEN CUSTOMER AND THE THIRD-PARTY OWNER OR DISTRIBUTOR OF THE THIRD-PARTY MATERIALS.

THE SERVICES, ASSESSMENT REPORT, AND ANY OTHER MATERIALS HEREUNDER ARE SOLELY PROVIDED TO CUSTOMER AND MAY NOT BE RELIED ON BY ANY OTHER PERSON OR FOR ANY PURPOSE NOT SPECIFICALLY IDENTIFIED IN THIS AGREEMENT, NOR MAY COPIES BE DELIVERED TO, ANY OTHER PERSON WITHOUT CERTIK'S PRIOR WRITTEN CONSENT IN EACH INSTANCE.

NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING

MATERIALS AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST CERTIK WITH RESPECT TO SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING MATERIALS.

THE REPRESENTATIONS AND WARRANTIES OF CERTIK CONTAINED IN THIS AGREEMENT ARE SOLELY FOR THE BENEFIT OF CUSTOMER. ACCORDINGLY, NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH REPRESENTATIONS AND WARRANTIES AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST CERTIK WITH RESPECT TO SUCH REPRESENTATIONS OR WARRANTIES OR ANY MATTER SUBJECT TO OR RESULTING IN INDEMNIFICATION UNDER THIS AGREEMENT OR OTHERWISE.

FOR AVOIDANCE OF DOUBT, THE SERVICES, INCLUDING ANY ASSOCIATED ASSESSMENT REPORTS OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.

About

Founded in 2017 by leading academics in the field of Computer Science from both Yale and Columbia University, CertiK is a leading blockchain security company that serves to verify the security and correctness of smart contracts and blockchain-based protocols. Through the utilization of our world-class technical expertise, alongside our proprietary, innovative tech, we’re able to support the success of our clients with best-in-class security, all whilst realizing our overarching vision; provable trust for all throughout all facets of blockchain.

CERTIK