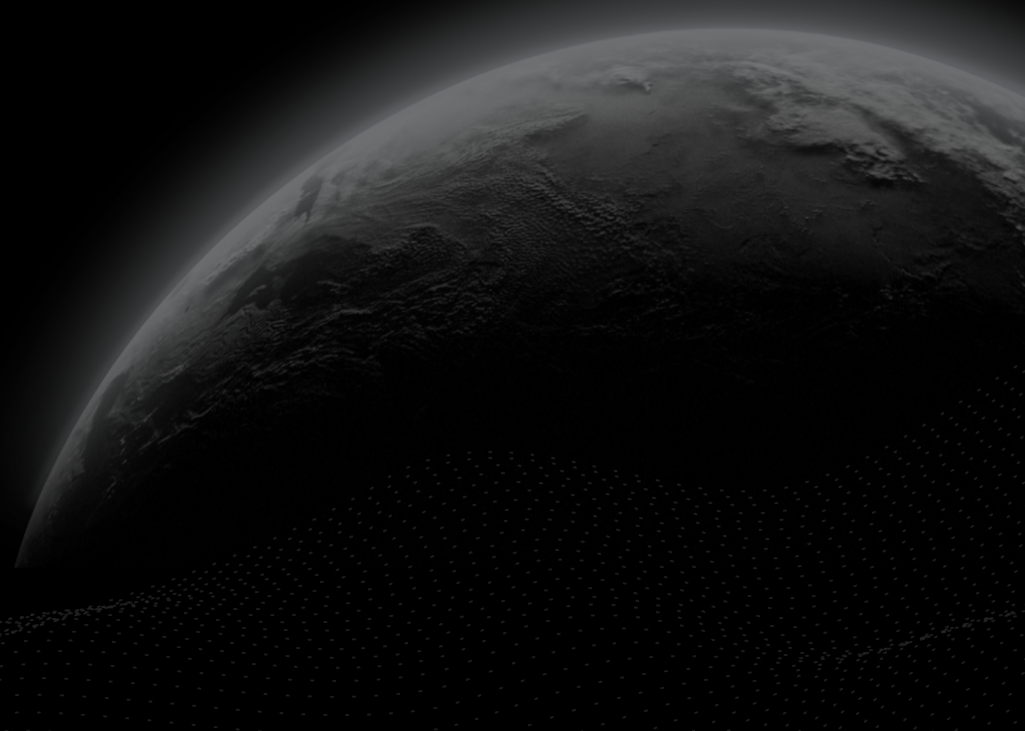
CERTIK

Security Assessment

Orbs single-nominator

CertiK Verified on Dec 15th, 2022



CertiK Verified on Dec 15th, 2022

Orbs single-nominator

The security assessment was prepared by CertiK, the leader in Web3.0 security.

Executive Summary

TYPES	ECOSYSTEM	METHODS
Other-Contract	TON	Manual Review

LANGUAGE	TIMELINE	KEY COMPONENTS
FunC	Delivered on 12/15/2022	N/A

CODEBASE

update 924658d0579c2692f919092127d3b8b70e569573

base 540d684c2de586d35bfdb85753143c6f9e1c376c

...View All

Vulnerability Summary

6	5	0	0	1	0	0
Total Findings	Resolved	Mitigated	Partially Resolved	Acknowledged	Declined	Unresolved

0	Critical		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.
0	Major		Major 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.
0	Medium		Medium risks may not pose a direct risk to users' funds, but they can affect the overall functioning of a platform.
5	Minor	4 Resolved, 1 Acknowledged	Minor 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.
1	Informational	1 Resolved	Informational errors are often recommendations to improve the style of the code or certain operations to fall within industry best practices. They usually do not affect the overall functioning of the code.

TABLE OF CONTENTS | ORBS SINGLE-NOMINATOR

CODEBASE | ORBS SINGLE-NOMINATOR

Repository

update 924658d0579c2692f919092127d3b8b70e569573

base 540d684c2de586d35bfdb85753143c6f9e1c376c

AUDIT SCOPE | ORBS SINGLE-NOMINATOR

2 files audited ● 1 file with Acknowledged findings ● 1 file without findings

ID	File	SHA256 Checksum
SIG	single-nominator.fc	84f485686c03d1b7bc076bef4d3d6e4482c33cbf7cd77902d7c1ebdcd7ed0376
SIL	single-nominator.fc	203f9e67c4af187c31c29101ddad45812f57c733876a50745d9270a9f3188f72

APPROACH & METHODS | ORBS SINGLE-NOMINATOR

This report has been prepared for Orbs to discover issues and vulnerabilities in the source code of the Orbs single-nominator project as well as any contract dependencies that were not part of an officially recognized library. A comprehensive examination has been performed, utilizing 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:

- Testing the smart contracts against both common and uncommon attack vectors;
- 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.

FINDINGS | ORBS SINGLE-NOMINATOR

6	0	0	0	5	1
Total Findings	Critical	Major	Medium	Minor	Informational

This report has been prepared to discover issues and vulnerabilities for Orbs single-nominator. Through this audit, we have uncovered 6 issues ranging from different severity levels. Utilizing the techniques of Manual Review to complement rigorous manual code reviews, we discovered the following findings:

ID	Title	Category	Severity	Status
SIG-01	`end_parse()` Is Missing	Coding Style	Minor	Resolved
SIG-02	Range Check Exception Is Thrown If `amount` Is Negative	Volatile Code	Minor	Resolved
SIG-03	`OP::NEW_STAKE` Message Construction Can Be Improved	Volatile Code	Minor	Resolved
SIG-04	Messages From Unknown Senders With Unrecognized Payloads Are Silently Accepted	Volatile Code	Minor	Resolved
SIG-05	Third Party Dependencies	Volatile Code	Minor	Acknowledged
SIG-06	Simple Transfer Is Accepted Before `load_data()` Validates The Initial State	Volatile Code	Informational	Resolved

SIG-01 | `end_parse()` IS MISSING

Category	Severity	Location	Status
Coding Style	Minor	single-nominator.fc (base): 38~39	Resolved

Description

`get_data()` contains 2 fields: `owner_address` and `validator_address`. The function `load_data()` reads all of them, however, it does not ensure that the slice is empty after that.

Recommendation

We recommend calling `ds.end_parse()` to ensure the slice doesn't contain more data.

SIG-02 RANGE CHECK EXCEPTION IS THROWN IF `amount` IS NEGATIVE

Category	Severity	Location	Status
Volatile Code	Minor	single-nominator.fc (base): 86~87	Resolved

Description

```
86              amount = min(amount, my_balance - msg_value - MIN_TON_FOR_STORAGE);
```

In case the contract's balance is less than `MIN_TON_FOR_STORAGE`, the `amount` can become negative. That will lead to a range check exception during `send_raw_message()`.

Recommendation

We recommend explicitly checking the `amount` correctness for better error reporting:

```
87      throw_unless(ERROR::INSUFFICIENT_BALANCE, amount > 0);
```

SIG-03 `OP::NEW_STAKE` MESSAGE CONSTRUCTION CAN BE IMPROVED

Category	Severity	Location	Status
Volatile Code	Minor	single-nominator.fc (base): 127~128	Resolved

Description

```
 127    send_msg(elector_address(), stake_amount, begin_cell().store_uint(op,
32).store_uint(query_id, 64).store_slice(msg).end_cell(), BOUNCEABLE,
MODE::SEND_MODE_REMAINING_AMOUNT); ;; bounceable, validator pays gas fees
```

The message sent to `elector-code` is built directly as the function argument. This decreases the code readability.

`op` sent to `elector-code` must be `OP::NEW_STAKE`. But `op` sent to `single-nominator` can be any. Passing `op` as an argument decreases the code maintainability.

Recommendation

We recommend constructing the message sent to `elector-code` in separate statements. We recommend using `OP::NEW_STAKE` explicitly instead of passing `op`. For example:

```
 126      cell payload = begin_cell().store_uint(OP::NEW_STAKE,
32).store_uint(query_id, 64).store_slice(msg).end_cell();
```

SIG-04 MESSAGES FROM UNKNOWN SENDERS WITH UNRECOGNIZED PAYLOADS ARE SILENTLY ACCEPTED

Category	Severity	Location	Status
Volatile Code	Minor	single-nominator.fc (base): 63~66	Resolved

Description

`recv_internal()` explicitly accepts the messages with empty `in_msg_body`. However, the messages with non-empty `in_msg_body` or from unauthorized senders are also implicitly accepted. This can lead to accidental errors.

Recommendation

We recommend explicitly `return ()` after each recognized command and rejecting all unsupported messages, like this:

```
136   ;; if op higher bit is zero, throw an exception (the message is an
137   ;; unsupported query) to bounce the message back to the sender
138   throw_unless(ERROR::UNSUPPORTED_QUERY, op & (1 << 31));
139   ;; do nothing for responses from the elector
```

Alleviation

[Orbs]: We think the recommendation has a higher risk. In case the elector will be upgraded in the future and the elector will change the returned format of the message it might result in a loss of funds in some scenarios. Therefore from our perspective, it's safer to not throw errors in this scenario.

[CertiK]: We took the **[Orbs]** position and marked the finding as Resolved.

SIG-05 | THIRD PARTY DEPENDENCIES

Category	Severity	Location	Status
Volatile Code	Minor	single-nominator.fc (base): 187~188	Acknowledged

Description

The contract is supposed to be interacted with by a third-party **mytonctrl** tool. The audit scope treats third-party entities as black boxes and assumes their functional correctness. However, the tool's functionality can be changed in the future, which may lead to incorrect `single-nominator` work.

Recommendation

We recommend constantly monitoring the functionality of **mytonctrl** tool to mitigate the side effects when unexpected changes are introduced.

Alleviation

[Orbs]: However, in this case there is no risk to staked funds, but you might need to fork **mytonctrl** code to support `single-nominator` api.

SIG-06 SIMPLE TRANSFER IS ACCEPTED BEFORE `load_data()` VALIDATES THE INITIAL STATE

Category	Severity	Location	Status
Volatile Code	Informational	single-nominator.fc (base): 75~76	Resolved

Description

In `recv_internal()` `load_data()` is performed after accepting of empty and bounced messages. In case the contract was initialized with incorrect initial state, it can still accept the stakes.

`load_data()` validates the storage is in correct format.

Recommendation

We recommend calling `load_data()` at the beginning of the function.

APPENDIX | ORBS SINGLE-NOMINATOR

Finding Categories

Categories	Description
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.

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 | CERTIK

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.

CertiK | Securing the Web3 World

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.