CERTIK

Security Assessment

TON Vesting

Aug 5th, 2022

Table of Contents

Summary

Overview

- Project Summary
- Audit Summary
- Vulnerability Summary
- Audit Scope

Findings

- 589-01 : Using of arbitrary integers in bitwise logical operations
- UNI-01 : `uint` values are stored as `int`
- UNI-02 : Function return value and argument types are not explicitly specified
- VES-01 : `send_raw_message()` is used in "Ignore errors" mode
- VES-02 : Improper Usage of `impure` Modifier
- VES-03 : Code Duplication

Appendix

Disclaimer

About

Summary

This report has been prepared for The Open Network to discover issues and vulnerabilities in the source code of the TON Vesting project. A comprehensive examination has been performed, utilizing Manual Review technique.

The auditing process pays special attention to the following considerations:

- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Thorough line-by-line manual review of the entire codebase by industry experts.

The security assessment resulted in findings that range from critical to informational. We recommend addressing these findings to ensure a high level of security standards and industry practices.

We suggest the following recommendations that could better serve the project from the security perspective:

- Document all the code functionality related to interaction with the users;
- Introduce the structure declaration concept into FunC;
- Introduce the constant declaration concept into FunC;
- Provide more comments per each function for better readability;
- Avoid using of `var` placeholder instead of explicit type specification;
- Introduce type specification in function declaration for arguments and return values.

Overview

Project Summary

Project Name	TON Vesting
Platform	TON
Language	FunC
Codebase	https://github.com/ton-blockchain/lockup-wallet-contract
Commit	base 589d65f7c6f1b23a6ac17fdac3740f1bf660efa5 update1 e3f46358ac3441da387f0b52a8096e7beb96f093

Audit Summary

Delivery Date	Aug 05, 2022 UTC
Audit Methodology	Manual Review

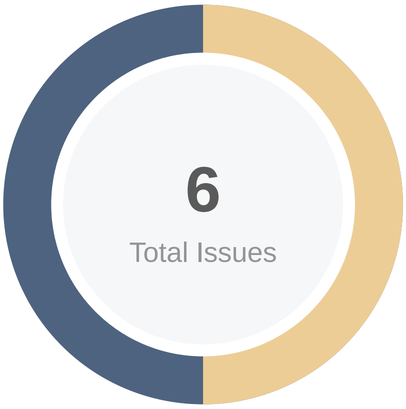
Vulnerability Summary

Vulnerability Level	Total	Pending	Declined	Acknowledged	Mitigated	Partially Resolved	Resolved
● Critical	0	0	0	0	0	0	0
● Major	0	0	0	0	0	0	0
● Medium	0	0	0	0	0	0	0
● Minor	3	0	0	1	0	1	1
● Informational	3	0	0	1	0	1	1
● Discussion	0	0	0	0	0	0	0

Audit Scope

ID	File	SHA256 Checksum
UNI	universal/uni-lockup-wallet.fc	a4134014c68a5b93312b3ef3ddb183c7061de82c495906dafb6cd7cb829ab8a2
VES	vesting/vesting-lockup-wallet.fc	2dadc76a69e2219b1ef22e3497c4ce579b5e0f1293ab6b9a6831d14f70a4a19d

Findings



🟥	**Critical**	**0** (0.00%)
🟧	**Major**	**0** (0.00%)
🟨	**Medium**	**0** (0.00%)
🟨	**Minor**	**3** (50.00%)
🟦	**Informational**	**3** (50.00%)
🟩	**Discussion**	**0** (0.00%)

ID	Title	Category	Severity	Status
589-01	Using Of Arbitrary Integers In Bitwise Logical Operations	Volatile Code	● Minor	Partially Resolved
UNI-01	`uint` Values Are Stored As `int`	Volatile Code	● Minor	ⓘ Acknowledged
UNI-02	Function Return Value And Argument Types Are Not Explicitly Specified	Coding Style	● Informational	ⓘ Acknowledged
VES-01	`send_raw_message()` Is Used In "Ignore Errors" Mode	Volatile Code	● Minor	✓ Resolved
VES-02	Improper Usage Of `impure` Modifier	Language Specific	● Informational	✓ Resolved
VES-03	Code Duplication	Coding Style	● Informational	Partially Resolved

589-01 | Using Of Arbitrary Integers In Bitwise Logical Operations

Category	Severity	Location	Status
Volatile Code	● Minor	universal/uni-lockup-wallet.fc (base): 151~152, 156~157; vesting/vesting-lockup-wallet.fc (base): 60~61	Partially Resolved

Description

`allow_elector` and `can_use_restricted` are 1-bit uint. However, they are used as part of logical expression. This can lead to accidental errors, like:

```
if (3 & 4) {
  ;; never happens
}
```

Recommendation

We recommend always using bool operands in bitwise logical operations, like `(allow_elector == 1)`.

Alleviation

[CertiK]: `uni-lockup-wallet.fc` was not updated.

UNI-01 | `uint` Values Are Stored As `int`

Category	Severity	Location	Status
Volatile Code	● Minor	universal/uni-lockup-wallet.fc (base): 53~55	ⓘ Acknowledged

Description

`seqno` and `subwallet_id` are saved into storage via `store_int()` but loaded via `load_uint()`. This can lead to exceptions in case of negative/too big values.

Recommendation

We recommend using of `store_uint()` for saving of `seqno` and `subwallet_id`.

UNI-02 | Function Return Value And Argument Types Are Not Explicitly Specified

Category	Severity	Location	Status
Coding Style	● Informational	universal/uni-lockup-wallet.fc (base): 16~17, 21~22, 33~34, 50~51	ⓘ Acknowledged

Description

Function declarations contain `_` instead of real return type. Argument types are omitted.

Recommendation

We recommend explicitly specifying the return value and argument types for a better code readability.

VES-01 | `send_raw_message()` Is Used In "Ignore Errors" Mode

Category	Severity	Location	Status
Volatile Code	● Minor	vesting/vesting-lockup-wallet.fc (base): 44~45, 68~69	✓ Resolved

Description

`mode = 3` means: +1 - sender pays fees, +2 - ignore errors. It is unclear, why "ignore errors" mode is enforced by the contract.

Recommendation

We recommend not restricting the mode values provided by the contract user or clarifying the intended behavior via code comments.

VES-02 | Improper Usage Of `impure` Modifier

Category	Severity	Location	Status
Language Specific	● Informational	vesting/vesting-lockup-wallet.fc (base): 22~23	✓ Resolved

Description

The function `recv_internal()` is defined as `impure`, but it does not modify the storage or throw an exception.

Recommendation

We recommend removing the `impure` modifier in the function definition.

VES-03 | Code Duplication

Category	Severity	Location	Status
Coding Style	● Informational	vesting/vesting-lockup-wallet.fc (base): 32~33, 55~59, 98~99, 99~103, 108~109	Partially Resolved

Description

Loading data from the storage is done by the identical code several times. `locked_amount` calculation is done by the identical code two times.

Recommendation

We recommend extracting the shared functionality into a separate function to improve the code maintainability. We recommend utilizing of `end_parse()` to ensure the data is in expected format.

Alleviation

[CertiK]: `locked_amount` calculation is done by the identical code two times.

Appendix

Finding Categories

Volatile Code

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

Language Specific

Language Specific findings are issues that would only arise within Solidity, i.e. incorrect usage of private or delete.

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