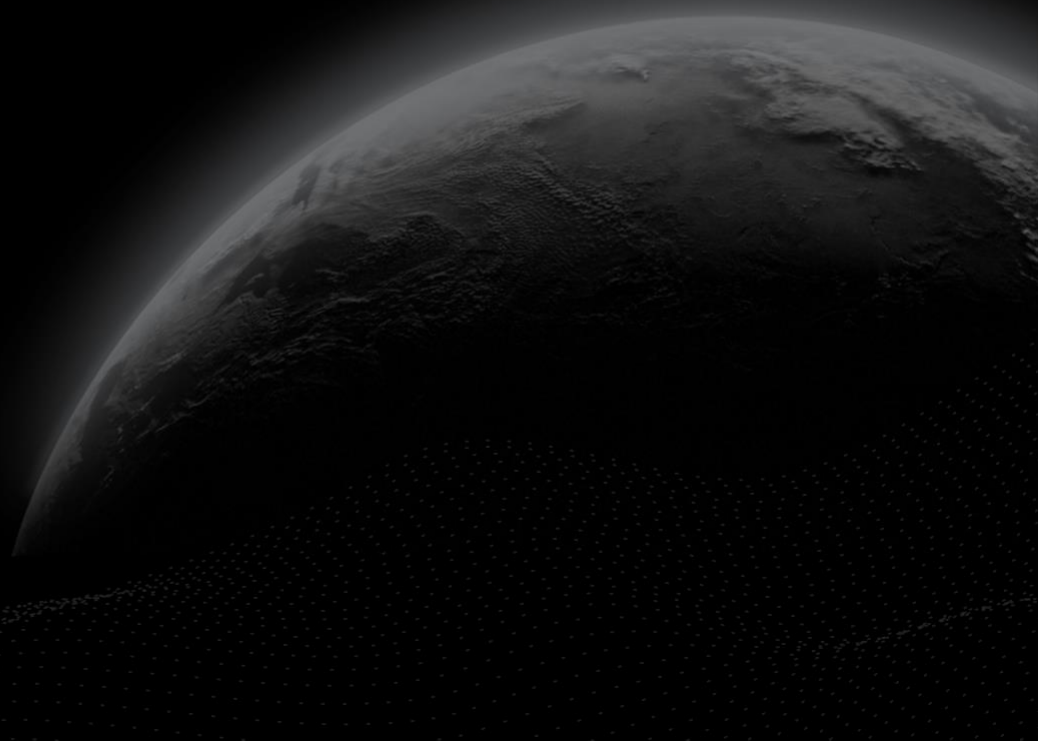
CERTIK

Security Assessment

XRPTurbo

CertiK Assessed on July 1st, 2026



CertiK Assessed on July 1st, 2026

XRPTurbo

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

Executive Summary

TYPES
Staking

ECOSYSTEM
XRPL

METHODS
Manual Review

LANGUAGE
Hooks

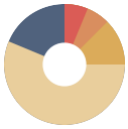
TIMELINE
Delivered on 07/01/2024

KEY COMPONENTS
N/A

CODEBASE
update
base
View All in Codebase Page

COMMITS
207cb3a713e24e2dcffc5e2aca47843df115c3eb
fc14d775d0641ad211f8b44c8cdd1dc1be134a7d
View All in Codebase Page

Vulnerability Summary



4	3	0	0	1	0
Total Findings	Resolved	Mitigated	Partially Resolved	Acknowledged	Declined

3 Informational	3 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.
1 Major	1 Acknowledged		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.

TABLE OF CONTENTS | XRPTurbo

CODEBASE | XRPTurbo

Repository

update

base

Commit

207cb3a713e24e2dcffc5e2aca47843df115c3eb

fc14d775d0641ad211f8b44c8cdd1dc1be134a7d

AUDIT SCOPE | XRPTurbo

6 files audited ● 6 files without findings

ID	Report	File	SHA256 Checksum
JET	xrp-turbo/systems	imports/multisig.fc	e5a63d94189cd4393c2c5bf0aadbb511d981325a457b483f9e25dfaf0697c19d3
NOM	xrp-turbo/systems	imports/nominator-proxy-utils.fc	183dabaa7027f486cbc96ceba19fa16bdd569931f74dacfe7b9550c4907dd486
UNS	xrp-turbo/systems	imports/withdraw-request.fc	7027f487af409166a8c43de45503e04fdf0317fba37bba472d958870dbfdc65af
ADM	xrp-turbo/systems	admin_multisig.fc	4b48618aa3cd4c50b457dafc5b16cbf4b61bc84ef40d66cf7736af1c334bb43
FIN	xrp-turbo/systems	financial.fc	383b438293ac6509ad760f6792cc41e993dba31b4cbba8360cef43b10cd46bfa
NOI	xrp-turbo/systems	nominator_proxy.fc	4b3218977225f2fdb1e1edf95ecf3242f87f015ff49a8aeb4eb04b269d63b486

APPROACH & METHODS | XRPTurbo

This report has been prepared for XRPTurbo to discover issues and vulnerabilities in the source code of the XRPTurbo project as well as any system 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 staking systems against both common and uncommon attack vectors.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring platform logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar systems 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 systems 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 systems that are verified in public;
- Provide more transparency on privileged activities once the protocol is live.

SLH-03 | CENTRALIZATION RISKS

Category	Severity	Location	Status
Centralization	**Major**	**financial.fc (base)**	**Acknowledged**

Description

In the system `financial` the role `admin_address` has authority over the functions:

- change `admin_address`, `commission_address`, and `transaction_address`
- change jetton `content`
- change `commission_factor`, which can be set even higher than 100%
- withdraw commission to `commission_address`
- update the `financial` code

The role `transaction_address` can send a transaction from `financial` to any address with any amount with any payload. `xrp_total_supply` is not updated in this case.

Any compromise to the `admin_address` and/or `transaction_address` may allow the hacker to take advantage of this authority and steal all the assets.

It is supposed that `admin_address` and `transaction_address` are controlled by a system with multi-signature functionality. `admin_address` also has a 12-hour timelock.

Recommendation

The risk describes the current project design and potentially makes iterations to improve the security operation and level of decentralization, which in most cases cannot be resolved entirely at the present stage. We advise the client to carefully manage the privileged account's private key to avoid any potential risks of being hacked.

Renouncing the ownership or removing the risky functionality can be considered fully resolved.

Alleviation

[Project Team]: Now `admin_address` and `transaction_address` are managed by multisigs.

SLI-04 | `wallet_id` VARIABLE IS SHADOWED

Category	Severity	Location	Status
Coding Style	Informational	transaction_multisig.fc	Resolved

Description

In `transaction_multisig` the inner scope variable `wallet_id` shadows another one in outer scope. This can lead to confusion.

Recommendation

We recommend avoiding variables shadowing.

SLU-09 | INACCURATE COMMENTS

Category	Severity	Location	Status
Coding Issue	Informational	admin_multisig.fc; nominator_proxy.fc	Resolved

Description

Some comments are inaccurate or outdated. In fact, nothing is triggered on an empty message. In fact, bounced messages are not ignored.

Recommendation

We recommend updating the comments.

SLU-10 | USAGE OF MAGIC NUMBERS

Category	Severity	Location	Status
Coding Style	Informational	admin_multisig.fc; nominator_proxy.fc; withrdaw_request.fc	Resolved

Description

Different magic numbers are used as-is in code.

- `financial` op-codes are used as numbers in `admin_multisig` , `nominator_proxy` , and `withdraw_request`
- Coded are used instead of `ACTION::DEPOSIT` / `ACTION::WITHDRAW` in `nominator_proxy`

Recommendation

We recommend declaring and using constants to improve code maintainability and readability.

OPTIMIZATIONS | XRPTurbo

ID	Title	Category	Severity	Status
SLB-02	No Reason To Parse `in_msg_full`	Fee Optimization	Optimization	Resolved

SLB-02 | NO REASON TO PARSE `in_msg_full`

Category	Severity	Location	Status
Gas Optimization	Optimization	nominator_proxy.fc	Resolved

Description

There is no reason to read `in_msg_full`. No values are used.

Recommendation

We recommend removing the redundant code.

APPENDIX | XRPTurbo

Finding Categories

Categories	Description
Fee Optimization	Fee 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.
Coding Style	Coding Style findings may not affect code behavior, but indicate areas where coding practices can be improved to make the code more understandable and maintainable.
Coding Issue	Coding Issue findings are about general code quality including, but not limited to, coding mistakes, compile errors, and performance issues.
Denial of Service	Denial of Service findings indicate that an attacker may prevent the program from operating correctly or responding to legitimate requests.
Inconsistency	Inconsistency findings refer to different parts of code that are not consistent or code that does not behave according to its specification.
Volatile Code	Volatile Code findings refer to segments of code that behave unexpectedly on certain edge cases and may result in vulnerabilities.
Logical Issue	Logical Issue findings indicate general implementation issues related to the program logic.
Centralization	Centralization findings detail the design choices of designating privileged roles or other centralized controls over the code.

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.