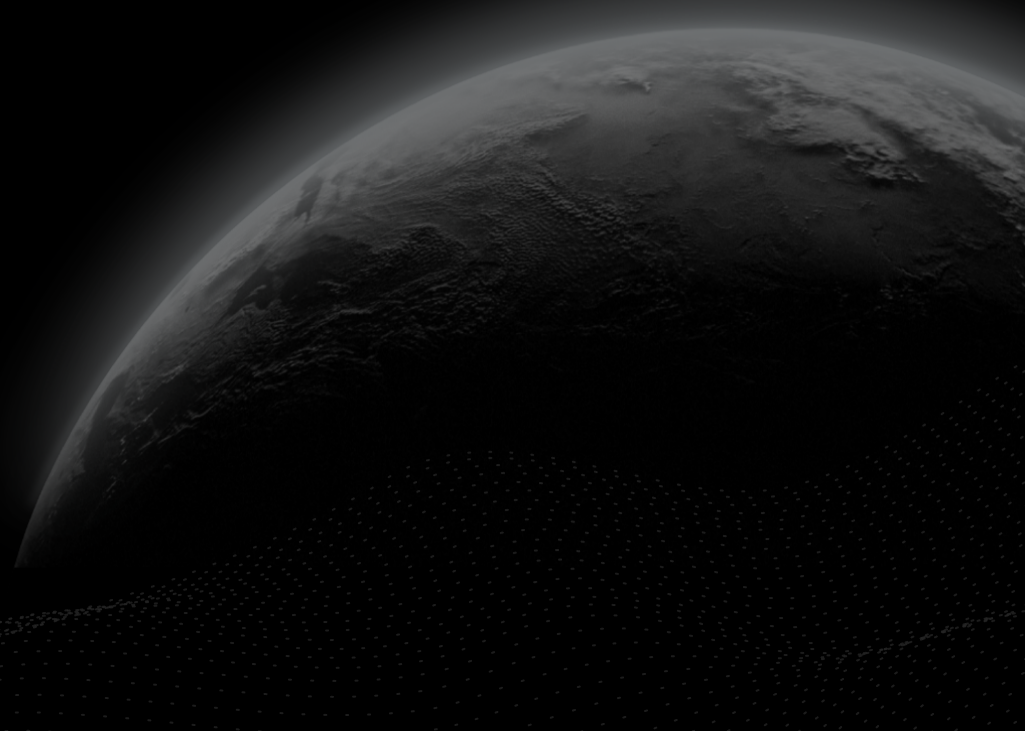
CERTIK

Security Assessment

TIP

CertiK Verified on Nov 18th, 2022



CertiK Verified on Nov 18th, 2022

TIP

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

Executive Summary

TYPES	ECOSYSTEM	METHODS
DeFi	Mixin Network	Manual Review, Static Analysis

LANGUAGE	TIMELINE	KEY COMPONENTS
Golang	Delivered on 11/18/2022	N/A

CODEBASE
https://github.com/MixinNetwork/tip/
...View All

COMMITS
fb379237ec89a5a96bd934f6256e2e6a18b2ad97
...View All

Vulnerability Summary

5	1	0	0	4	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.
1	Major	1 Resolved	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.
1	Medium	1 Acknowledged	Medium risks may not pose a direct risk to users' funds, but they can affect the overall functioning of a platform.
0	Minor		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.
3	Informational	3 Acknowledged	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 | TIP

CODEBASE | TIP

Repository

https://github.com/MixinNetwork/tip/

Commit

fb379237ec89a5a96bd934f6256e2e6a18b2ad97

AUDIT SCOPE | TIP

16 files audited ● 2 files with Acknowledged findings ● 1 file with Resolved findings ● 13 files without findings

ID	File	SHA256 Checksum
MNT	messenger/mixin.go	eb27a1d45106a85ab6124ffe12099d6d1419e082f495a723cc98fc60540d5451
MNO	logger/log.go	22f440abaee308ed167f43fd6d01ede1b1cb3d56a9f6a59a862316271d92cbe9
MNU	store/badger.go	92e21633adeeb9e65453de923413b7d7972d2f04eef6e9437e92e0a338a0a90d
MNB	main.go	ef03dfd1ae5087228685027027e055970c9fa37a045555d76f1f5d1e3ed8a041
MNH	store/interface.go	8febd86725bcb9768882b31084f4341cd2a75f68fffc763e4d63004d72235a71
MNI	messenger/interface.go	fa0fd3e81127d3f126de7f0aaf9f9a93d79e2d1ea6ce8438bc1c252e34a34068
MNG	messenger/errors.go	4ce1662a212a4aa112c6bfcbe2a0744d1f8b52fe0375b1262fa2d7296b3c0244
MNW	keeper/guard.go	a364aaaa79308e5aed0041b53b42b5c59cb895f062d23f4c0ce78904c5fd12f8
MNE	crypto/bls.go	2ab3956025f34699acab95f26e776e7884c8e77566ce8027407298d8ab78d0a3
MBU	crypto/aes.go	d574153ecc71779d3225611b27074c1e48fa1dc06e739fd1222dd286e414c96f
MBT	config/example.json	bce14552cf1d9be345f9e30d3eceff65370cb2965ec32dc01b946d8409bb9992
MBI	config/example.toml	585f21d8fa5826402c803a6134a2d70ae90be1f0b61512f3eed6e9ee7bb19cbb
MBG	config/reader.go	d4311792a9ae5faaaa254ae3c1a84f394c6912a568f7501d7513209ededcef6e
MBR	api/errors.go	9749e1b2c23c06dae2f31874a13109aeeda3bd20db2c2486f702db3682436827
MBO	api/http.go	9cb176c277a3c206bd7dde6a6fcf4240b2cf52673d62c45d05d1d6bbf8c91c86
MBW	api/json.go	e7149e837e04b2adf7f020f34f99a9716ecbcdb9ec4e9e8f572e3bbd5861ced4

APPROACH & METHODS | TIP

This report has been prepared for MixinNetwork to discover issues and vulnerabilities in the source code of the TIP 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 and Static Analysis 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 | TIP

5	0	1	1	0	3
Total Findings	Critical	Major	Medium	Minor	Informational

This report has been prepared to discover issues and vulnerabilities for TIP. Through this audit, we have uncovered 5 issues ranging from different severity levels. Utilizing the techniques of Manual Review & Static Analysis to complement rigorous manual code reviews, we discovered the following findings:

ID	Title	Category	Severity	Status
GLOBAL-01	Third Party Dependencies	Volatile Code	Medium	Acknowledged
MNU-01	Potential Incorrect Logic	Logical Issue	Major	Resolved
MNO-01	Unused Function	Volatile Code	Informational	Acknowledged
MNT-01	Unused Parameters	Coding Style	Informational	Acknowledged
MNT-02	Unimplemented Functions	Logical Issue	Informational	Acknowledged

GLOBAL-01 | THIRD PARTY DEPENDENCIES

Category	Severity	Location	Status
Volatile Code	Medium		Acknowledged

Description

The contract is serving as the underlying entity to interact with third party **drand/kyber**, **fox-one/mixin-sdk-go**, **badger** protocols. The scope of the audit treats 3rd party entities as black boxes and assumes their functional correctness. However, in the real world, 3rd parties can be compromised and this may lead to lost or stolen assets. Additionally, upgrades of 3rd parties can possibly create severe impacts, such as increasing fees of 3rd parties, migrating to new LP pools, etc.

Recommendation

We understand that the business logic of this protocol requires interaction with **drand/kyber**, **fox-one/mixin-sdk-go**, **badger**, etc. We encourage the team to constantly monitor the statuses of 3rd parties to mitigate the side effects when unexpected activities are observed.

Alleviation

The team acknowledged the finding.

MNU-01 | POTENTIAL INCORRECT LOGIC

Category	Severity	Location	Status
Logical Issue	Major	store/badger.go: 285~287	Resolved

Description

```
282     cb, err := readKey(txn, badgerKeyPrefixCounter, assignor)
283     if err != nil {
284         return err
285     } else if cb != nil {
286         counter = int(binary.BigEndian.Uint64(cb))
287     } else {
288         counter = 1
289     }
```

The `counter` is the data stored in the badger whose prefix is `badgerKeyPrefixCounter`.

In our opinion, in code `badger.go` #L232, the `counter` of `assignor` is increased every time the function `WriteAssignee()` is called.

However, in the function `writeSignRequest()` (`badger.go` #L286-L288), this part of the code we understand is to initialize a counter if the counter corresponding to the assignor does not exist in the badger. But why assign 1 to the counter? If the logic of this part of the code requires an incremental operation on the counter why don't line 286 add 1 to the counter?

Recommendation

Please review the logic to ensure it meets design intent.

Alleviation

[Mixin]: Counter means the number of key an identity has used in the node, thus the first counter returned is 1 after an identity assignor created. counter is only increased whenever a new key created, i.e. WriteAssignee some new comments from https://github.com/MixinNetwork/tip/blob/main/store/badger.go#L294

MNO-01 | UNUSED FUNCTION

Category	Severity	Location	Status
Volatile Code	Informational	logger/log.go: 19~21, 39~41, 47~49	Acknowledged

Description

These functions are not used but implemented.

Recommendation

We advise removing it if there is no plan for further usage.

Alleviation

The team acknowledged the finding.

MNT-01 | UNUSED PARAMETERS

Category	Severity	Location	Status
Coding Style	Informational	messenger/mixin.go: 85	Acknowledged

Description

The linked parameters are never used.

Recommendation

We recommend the client to remove them if there is no plan for further usage.

Alleviation

The team acknowledged the finding.

MNT-02 | UNIMPLEMENTED FUNCTIONS

Category	Severity	Location	Status
Logical Issue	Informational	messenger/mixin.go: 112~114	Acknowledged

Description

The function `onAckReceipt()` is used but not implemented.

Recommendation

Please implement these functions before deploying.

Alleviation

The team acknowledged the finding.

APPENDIX | TIP

Finding Categories

Categories	Description
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.
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.