CERTIK

Security Assessment

Equito Finance

CertiK Verified on Nov 28th, 2022

CertiK Verified on Nov 28th, 2022

Equito Finance

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

Executive Summary

TYPES	ECOSYSTEM	METHODS
Bridge	Algorand	Manual Review, Static Analysis
LANGUAGE	**TIMELINE**	**KEY COMPONENTS**
Python	Delivered on 11/28/2022	N/A

CODEBASE
https://git.mobilesoft.it/equito-finance/contracts/equito-contract-v1
...View All

COMMITS
3fd7e2ec167c372120e551dc88cd108413864c7b
...View All

Vulnerability Summary

5	2	2	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.
2	Medium	2 Mitigated	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	2 Resolved, 1 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 | EQUITO FINANCE

CODEBASE | EQUITO FINANCE

Repository

https://git.mobilesoft.it/equito-finance/contracts/equito-contract-v1

Commit

3fd7e2ec167c372120e551dc88cd108413864c7b

AUDIT SCOPE | EQUITO FINANCE

6 files audited ● 1 file with Acknowledged findings ● 1 file with Mitigated findings ● 4 files without findings

ID	File	SHA256 Checksum
BMC	project/equito/contracts/bridge/BaseMinter.py	6c0ab4e53cfad010014fef04a5d9c81cb9a67472035c73c893fb928131756db9
VCK	project/equito/contracts/bridge/Vault.py	cbfba14a05c2f09aeba4d969dbc7621b9bd435b68f7359f17d720bc312599b3f
BNB	project/equito/contracts/bridge/BNBMinter.py	d1eb3ebe5ab84b08bb740d48c41f1e26ea5c44ab230b61372c6fa86a4b2d8b63
BUM	project/equito/contracts/bridge/BnbUsdcMinter.py	409f270e708dbf4c365e6d7815243b9b6e0940a58c73d90bc206d93c0fafa732
ETH	project/equito/contracts/bridge/ETHMinter.py	6ceac18cef9f971272cf87c8df5e77dfe1703e0ef4486d5d19cc7f3d2876b253
EUM	project/equito/contracts/bridge/EthUsdcMinter.py	9ac0882087b733b4ddf7e0fa72c4ef2885c0fda942e6e55e80f16ea97496dde8

APPROACH & METHODS | EQUITO FINANCE

This report has been prepared for Equito Finance to discover issues and vulnerabilities in the source code of the Equito Finance 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 | EQUITO FINANCE

5	0	0	2	0	3
Total Findings	Critical	Major	Medium	Minor	Informational

This report has been prepared to discover issues and vulnerabilities for Equito Finance . 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
BMC-01	**Centralization Related Risks**	**Centralization / Privilege**	**Medium**	**Mitigated**
VCK-01	**Centralization Related Risks**	**Centralization / Privilege**	**Medium**	**Mitigated**
BMC-02	Missing IPFS Check	Volatile Code	Informational	Acknowledged
BMC-03	`on_burn` Sends Burned Token To Contract Address	Volatile Code	Informational	Resolved
VCK-02	Unused Functions	Logical Issue	Informational	Resolved

BMC-01 | CENTRALIZATION RELATED RISKS

Category	Severity	Location	Status
Centralization / Privilege	**Medium**	**project/equito/contracts/bridge/BaseMinter.py: 90**	**Mitigated**

Description

In the contract BaseMinter.py, the role admin has authority over the following functions:

- on_mint Any compromise to the admin account may allow a hacker to take advantage of this authority and send the created asset to addresses that has already opted in.

Recommendation

The risk describes the current project design and potentially makes iterations to improve in the security operation and level of decentralization, which in most cases cannot be resolved entirely at the present stage. We recommend carefully managing the privileged account's private key to avoid any potential risks of being hacked. In general, we strongly recommend centralized privileges or roles in the protocol be improved via a decentralized mechanism or smart-contract-based accounts with enhanced security practices, e.g., multi-signature wallets.

Indicatively, here are some feasible suggestions that would also mitigate the potential risk at a different level in terms of short-term, long-term and permanent:

Long Term:

Multi sign (⅔, ⅗) *mitigate* by avoiding a single point of key management failure.

- Assignment of privileged roles to multi-signature wallets to prevent a single point of failure due to the private key compromised;
  AND
- A medium/blog link for sharing the multi-signers addresses information with the public audience.

Permanent:

Renouncing the ownership or removing the function can be considered *fully resolved*.

- Renounce the ownership and never claim back the privileged roles;
  OR
- Remove the risky functionality.

Alleviation

[Equito Finance Team]: All transactions (create contracts, call contract functions...) of bridge are not signed by admin account, and they are signed by multi-signature wallet(2 of 3).

Multi-signature wallet is generated in backend, and it is used to sign all bridge transactions.

And individual private key of accounts that compose up the multi-sig wallet are stored in the individual backend instances.

Although one backend instance is hacked, the other backend instances are safe, and the bridge transactions are safe, too.

We are using Azure secret key vault service to store the private keys, its access control will be strictly done by management team.

VCK-01 | CENTRALIZATION RELATED RISKS

Category	Severity	Location	Status
Centralization / Privilege	**Medium**	**project/equito/contracts/bridge/Vault.py: 91~125**	**Mitigated**

Description

In the contract BaseMinter.py, the role admin has authority over the following functions:

- on_release_algo
- on_release_usdc Any compromise to the admin account may allow a hacker to take advantage of this authority and send ALGO or USDC to other addresses.

Recommendation

The risk describes the current project design and potentially makes iterations to improve in the security operation and level of decentralization, which in most cases cannot be resolved entirely at the present stage. We recommend carefully managing the privileged account's private key to avoid any potential risks of being hacked. In general, we strongly recommend centralized privileges or roles in the protocol be improved via a decentralized mechanism or smart-contract-based accounts with enhanced security practices, e.g., multi-signature wallets.

Indicatively, here are some feasible suggestions that would also mitigate the potential risk at a different level in terms of short-term, long-term and permanent:

Long Term:

Multi sign (⅔, ⅗) *mitigate* by avoiding a single point of key management failure.

- Assignment of privileged roles to multi-signature wallets to prevent a single point of failure due to the private key compromised;
  AND
- A medium/blog link for sharing the multi-signers addresses information with the public audience.

Permanent:

Renouncing the ownership or removing the function can be considered *fully resolved*.

- Renounce the ownership and never claim back the privileged roles;
  OR
- Remove the risky functionality.

Alleviation

[Equito Finance Team]: on_release_algo and on_release_usdc transactions are signed by multi-sig wallet.

It is the same with BMC-01 CENTRALIZATION RELATED RISKS issue.

BMC-02 | MISSING IPFS CHECK

Category	Severity	Location	Status
Volatile Code	Informational	project/equito/contracts/bridge/BaseMinter.py: 14	Acknowledged

Description

The `ASSET_URL` is using https instead of a valid IPFS location.

Recommendation

It's recommended to use IPFS for NFT token metadata rather than HTTP/HTTPS. For HTTP/HTTPS, the domain and web server owner can change token metadata at will to dramatically affect token value.

Reference: https://developer.algorand.org/solutions/securely-share-files-algorand-ipfs/

Alleviation

[Equito Finance Team]:

The ASSET_URL is not a real asset URL.

It is only normal string.

So it doesn't need to use IPFS for NFT token metadata.

BMC-03 | `on_burn` SENDS BURNED TOKEN TO CONTRACT ADDRESS

Category	Severity	Location	Status
Volatile Code	Informational	project/equito/contracts/bridge/BaseMinter.py: 107	Resolved

Description

We noticed that tokens being burned are sent to the contract address, which is also the reserve address. Note that the burn operation is reversible in this case. The total supply is not changed in this case.

Reference: https://forum.algorand.org/t/stablecoin-how-to-burn-the-asset-and-update-the-supply/1838

Recommendation

We would like the client to confirm that this is the intended design.

Alleviation

[Equito Finance Team]:

Algorand can't create the asset dinamically.

The asset is created only once, and the initial amount of asset is fixed.

So burned assets are returned to the contract address, and it is reused later.

We confirm that this is intended by design.

VCK-02 | UNUSED FUNCTIONS

Category	Severity	Location	Status
Logical Issue	Informational	project/equito/contracts/bridge/Vault.py: 81~89	Resolved

Description

The function `on_lock_algo` and `on_lock_usdc` are declared but never used in the contract.

Recommendation

We advise the client to remove or comment out the functions.

Alleviation

Functions are removed in commit 3fd7e2ec167c372120e551dc88cd108413864c7b.

APPENDIX | EQUITO FINANCE

Finding Categories

Categories	Description
Centralization / Privilege	Centralization / Privilege findings refer to either feature logic or implementation of components that act against the nature of decentralization, such as explicit ownership or specialized access roles in combination with a mechanism to relocate funds.
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.

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.