CERTIK

MEXAS

Security Assessment

CertiK Assessed on May 12th, 2026





CertiK Assessed on May 12th, 2026

MEXAS

The security assessment was prepared by CertiK.

Executive Summary

TYPES	ECOSYSTEM	METHODS
ERC-20	EVM Compatible	Formal Verification, Manual Review, Static Analysis

LANGUAGE	TIMELINE
Solidity	Preliminary comments published on 10/14/2025 Final report published on 05/12/2026

Vulnerability Summary



3	0	2	0	1	0
Total Findings	Resolved	Multi-Sig	Partially Resolved	Acknowledged	Declined

2	Centralization	2 Multi-Sig	Centralization findings highlight privileged roles & functions and their capabilities, or instances where the project takes custody of users' assets.
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 may include logical errors that, under specific circumstances, could result in fund losses or loss of project control.
0	Medium		Medium risks may not pose a direct risk to users' funds, but they can affect the overall functioning of a platform.
1	Minor	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.
0	Informational		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 | MEXAS

Audit Summary

Executive Summary

Vulnerability Summary

Codebase

Audit Scope

Approach & Methods

Findings

MEX-02 : Centralized Control Of Contract Upgrade

MEX-03 : Centralization Risks In MEXAS.Sol

MEX-04 : Local Variable Shadowing

Appendix

Disclaimer

CODEBASE | MEXAS

Repository

https://github.com/mexas-io/mexas-stablecoin

Commit

02a21eaecb5fc7323ce24e3576c81377d8b6e9af

bb91ec389122f54b40ab7670fb97e3c610ecdb90

AUDIT SCOPE | MEXAS

mexas-io/mexas-stablecoin

contracts/MEXAS.sol

APPROACH & METHODS | MEXAS

This audit was conducted for MEXAS to evaluate the security and correctness of the smart contracts associated with the MEXAS project. The assessment included a comprehensive review of the in-scope smart contracts. The audit was performed using a combination of Formal Verification, Manual Review, and Static Analysis.

The review process emphasized the following areas:

- Architecture review and threat modeling to understand systemic risks and identify design-level flaws.
- Identification of vulnerabilities through both common and edge-case attack vectors.
- Manual verification of contract logic to ensure alignment with intended design and business requirements.
- Dynamic testing to validate runtime behavior and assess execution risks.
- Assessment of code quality and maintainability, including adherence to current best practices and industry standards.

The audit resulted in findings categorized across multiple severity levels, from informational to critical. To enhance the project's security and long-term robustness, we recommend addressing the identified issues and considering the following general improvements:

- Improve code readability and maintainability by adopting a clean architectural pattern and modular design.
- Strengthen testing coverage, including unit and integration tests for key functionalities and edge cases.
- Maintain meaningful inline comments and documentations.
- Implement clear and transparent documentation for privileged roles and sensitive protocol operations.
- Regularly review and simulate contract behavior against newly emerging attack vectors.

FINDINGS | MEXAS



3	0	2	0	0	1	0
Total Findings	Critical	Centralization	Major	Medium	Minor	Informational

This report has been prepared for MEXAS to identify potential vulnerabilities and security issues within the reviewed codebase. During the course of the audit, a total of 3 issues were identified. Leveraging a combination of Formal Verification, Manual Review & Static Analysis the following findings were uncovered:

ID	Title	Category	Severity	Status
MEX-02	**Centralized Control Of Contract Upgrade**	**Centralization**	**Centralization**	**3/5 Multi-Sig**
MEX-03	**Centralization Risks In MEXAS.Sol**	**Centralization**	**Centralization**	**3/5 Multi-Sig**
MEX-04	Local Variable Shadowing	Coding Style	Minor	Acknowledged

MEX-02 | Centralized Control Of Contract Upgrade

Category	Severity	Location	Status
Centralization	**Centralization**	**contracts/MEXAS.sol: 15**	**3/5 Multi-Sig**

Description

In the contract MEXAS, the role `owner` has the authority to update the implementation contract behind the MEXAS contract.

Any compromise to the `owner` account may allow a hacker to take advantage of this authority and change the implementation contract which is pointed by proxy and therefore execute potential malicious functionality in the implementation contract.

Recommendation

We recommend that the team make efforts to restrict access to the admin of the proxy contract. A strategy of combining a time-lock and a multi-signature (⅔, ⅗) wallet can be used to prevent a single point of failure due to a private key compromise. In addition, the team should be transparent and notify the community in advance whenever they plan to migrate to a new implementation contract.

Here are some feasible short-term and long-term suggestions that would mitigate the potential risk to a different level and suggestions that would permanently fully resolve the risk.

Short Term:

A combination of a time-lock and a multi signature (⅔, ⅗) wallet mitigate the risk by delaying the sensitive operation and avoiding a single point of key management failure.

- A time-lock with reasonable latency, such as 48 hours, for awareness of privileged operations;
  AND
- Assignment of privileged roles to multi-signature wallets to prevent a single point of failure due to a private key compromised;
  AND
- A medium/blog link for sharing the time-lock contract and multi-signers addresses information with the community.

For remediation and mitigated status, please provide the following information:

- Provide the deployed time-lock address.
- Provide the **gnosis** address with **ALL** the multi-signer addresses for the verification process.
- Provide a link to the **medium/blog** with all of the above information included.

Long Term:

A combination of a time-lock on the contract upgrade operation and a DAO for controlling the upgrade operation mitigate the contract upgrade risk by applying transparency and decentralization.

- A time-lock with reasonable latency, such as 48 hours, for community awareness of privileged operations;
  AND
- Introduction of a DAO, governance, or voting module to increase decentralization, transparency, and user involvement;
  AND
- A medium/blog link for sharing the time-lock contract, multi-signers addresses, and DAO information with the community.

For remediation and mitigated status, please provide the following information:

- Provide the deployed time-lock address.
- Provide the **gnosis** address with **ALL** the multi-signer addresses for the verification process.
- Provide a link to the **medium/blog** with all of the above information included.

Permanent:

Renouncing ownership of the `admin` account or removing the upgrade functionality can *fully* resolve the risk.

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

Note: we recommend the project team consider the long-term solution or the permanent solution. The project team shall make a decision based on the current state of their project, timeline, and project resources.

Alleviation

[MEXAS, 05/11/2026]:

Ethereum Mainnet:

The MEXAS contract has transferred the ownership to a Gnosis Safe contract with 3/5 signers in the sensitive function signing process.

- Grant Role transaction hash for Gnosis Safe: https://etherscan.io/tx/0x12800fe905b49aca55d6ba5284f78ea57b18dc886899490c519943ba3e9efde6, Gnosis safe contract address: https://etherscan.io/address/0x82c40c2921dc724c36fa89d0d6014c6d3dfb7c08#code
- The 3/5 multisign addresses:
  1. EOA:0x26bD65AE120ed6a169Bb6cc5AAd2db23fb9d7D8F

2. EOA:0x3e7Dd8dC8C9bf7Ea1139f626a4c62A8dd97eA15c
3. EOA:0x1324CC2bB8Ac1dD809D7d1ECF87FE3387cfD2a9d
4. EOA:0x9050401fd8e03dDB82df79Fc3A280feD7d360F71
5. EOA:0x29d6206a6f3d4d74Edf0Ac36a9Fe0A3f8733cd25

Arbitrum Mainnet:

The MEXAS contract has transferred the ownership to a Gnosis Safe contract with 3/5 signers in the sensitive function signing process.

- Grant Role transaction hash for Gnosis Safe: https://arbiscan.io/tx/0x29d2871ebd1ce592de01e0419460c34846a8dbe85075fb68a2bc5adb2505de7b, Gnosis safe contract address: https://arbiscan.io/address/0x7851bB23D54Bc032A3eb82F4cCCCAD4287Ab62a4
- The 3/5 multisign addresses:
  1. EOA:0x26bD65AE120ed6a169Bb6cc5AAd2db23fb9d7D8F
  2. EOA:0x3e7Dd8dC8C9bf7Ea1139f626a4c62A8dd97eA15c
  3. EOA:0x1324CC2bB8Ac1dD809D7d1ECF87FE3387cfD2a9d
  4. EOA:0x9050401fd8e03dDB82df79Fc3A280feD7d360F71
  5. EOA:0x29d6206a6f3d4d74Edf0Ac36a9Fe0A3f8733cd25

Avalanche Mainnet:

The MEXAS contract has transferred the ownership to a Gnosis Safe contract with 3/5 signers in the sensitive function signing process.

- Grant Role transaction hash for Gnosis Safe: https://snowtrace.io/tx/0xf5efae3565afc48960273e1e1275da955415c9b7e07f113c077c2b62730980fe?chainid=43114, Gnosis safe contract address: https://snowtrace.io/address/0x524A6E0421D9bF2524d9f13595df1aefE2571A6A
- The 3/5 multisign addresses:
  1. EOA:0x26bD65AE120ed6a169Bb6cc5AAd2db23fb9d7D8F
  2. EOA:0x3e7Dd8dC8C9bf7Ea1139f626a4c62A8dd97eA15c
  3. EOA:0x1324CC2bB8Ac1dD809D7d1ECF87FE3387cfD2a9d
  4. EOA:0x9050401fd8e03dDB82df79Fc3A280feD7d360F71
  5. EOA:0x29d6206a6f3d4d74Edf0Ac36a9Fe0A3f8733cd25

Base Mainnet:

The MEXAS contract has transferred the ownership to a Gnosis Safe contract with 3/5 signers in the sensitive function signing process.

- Grant Role transaction hash for Gnosis Safe: https://basescan.org/tx/0x94fc630393429abcb8924812099ec4f7ac3a55cef512ab8af2097b865ed2a0f7, Gnosis safe contract address: https://basescan.org/address/0x72c41E6A7F83dB2557092814299Ea5129111Cf75
- The 3/5 multisign addresses:
  1. EOA:0x26bD65AE120ed6a169Bb6cc5AAd2db23fb9d7D8F
  2. EOA:0x3e7Dd8dC8C9bf7Ea1139f626a4c62A8dd97eA15c
  3. EOA:0x1324CC2bB8Ac1dD809D7d1ECF87FE3387cfD2a9d
  4. EOA:0x9050401fd8e03dDB82df79Fc3A280feD7d360F71
  5. EOA:0x29d6206a6f3d4d74Edf0Ac36a9Fe0A3f8733cd25

BSC Mainnet:

The MEXAS contract has transferred the ownership to a Gnosis Safe contract with 3/5 signers in the sensitive function signing process.

- Grant Role transaction hash for Gnosis Safe: https://bscscan.com/tx/0xe63a3de6373767ea4dea5cdc1f0237b75c9ad8f2d5665d2c0c9bb7d399e75af4, Gnosis safe contract address: https://bscscan.com/address/0x42b8A305F548FA47Dd2309BC54198fcA0C9A15eA#code
- The 3/5 multisign addresses:
  1. EOA:0x26bD65AE120ed6a169Bb6cc5AAd2db23fb9d7D8F
  2. EOA:0x3e7Dd8dC8C9bf7Ea1139f626a4c62A8dd97eA15c
  3. EOA:0x1324CC2bB8Ac1dD809D7d1ECF87FE3387cfD2a9d
  4. EOA:0x9050401fd8e03dDB82df79Fc3A280feD7d360F71
  5. EOA:0x29d6206a6f3d4d74Edf0Ac36a9Fe0A3f8733cd25

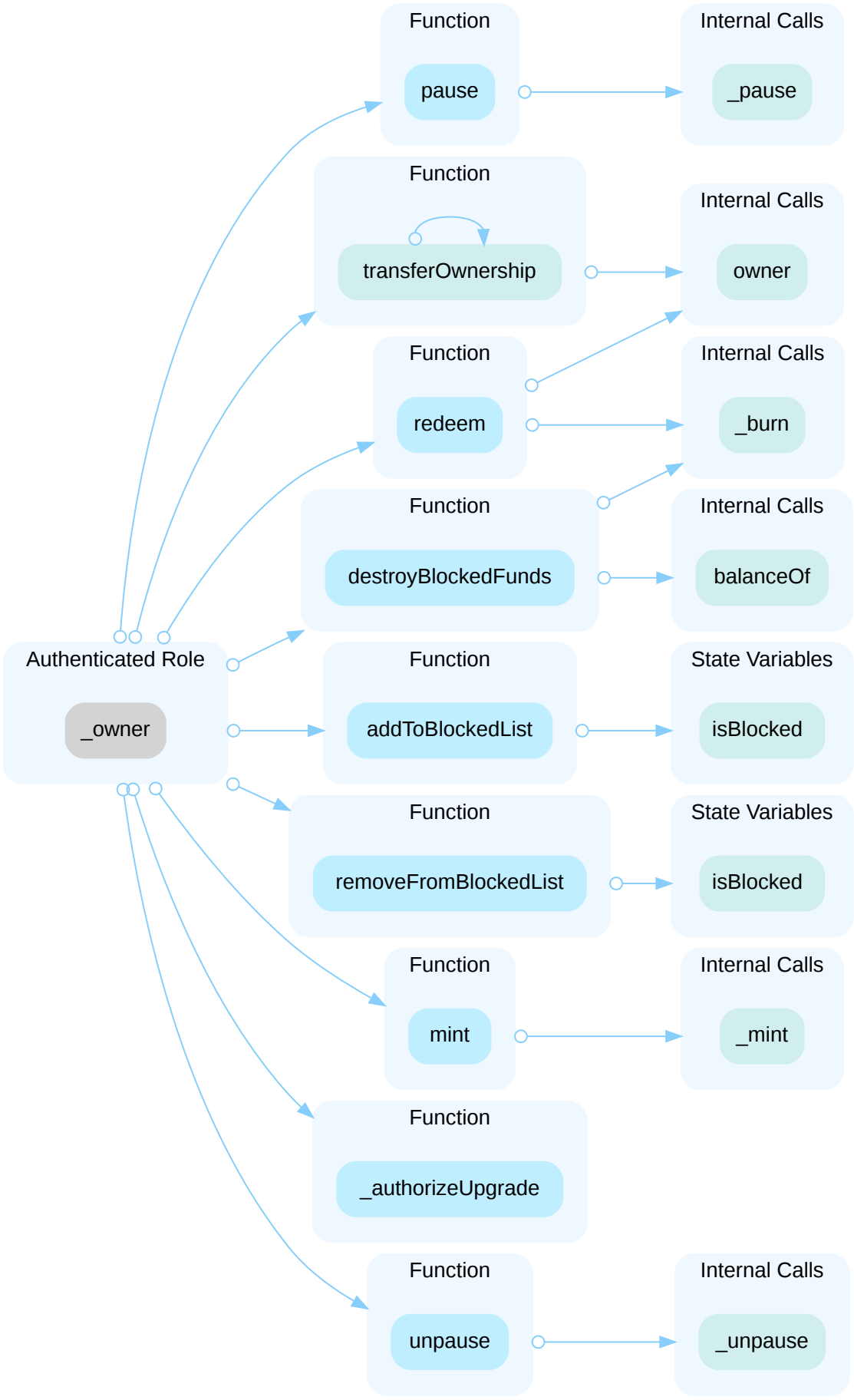
[CertiK, 05/12/2026]: While this strategy has indeed reduced the risk, it's crucial to note that it has not completely eliminated it. CertiK strongly encourages the project team to periodically revisit the private key security management of all above-listed addresses.

MEX-03 | Centralization Risks In MEXAS.Sol

Category	Severity	Location	Status
Centralization	**Centralization**	**contracts/MEXAS.sol**	**3/5 Multi-Sig**

Description

In the contract `MEXAS` the role `_owner` has authority over the functions shown in the diagram below. Any compromise to the owner account may allow an attacker to blacklist or unblacklist users, arbitrarily mint or burn supply (including seizing blocked balances), halt or resume transfers, reassign ownership, and upgrade the implementation to malicious logic, placing full control of token issuance, circulation, and contract behavior in a single centralized authority.


Function
pause
Internal Calls
_pause
Function
transferOwnership
Internal Calls
owner
Function
redeem
Internal Calls
_burn
Function
destroyBlockedFunds
Internal Calls
balanceOf
Authenticated Role
_owner
Function
addToBlockedList
State Variables
isBlocked
Function
removeFromBlockedList
State Variables
isBlocked
Function
mint
Internal Calls
_mint
Function
_authorizeUpgrade
Function
unpause
Internal Calls
_unpause

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 advise the client to carefully manage 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., multisignature 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:

Short Term:

Timelock and Multi sign (⅔, ⅗) combination *mitigate* by delaying the sensitive operation and avoiding a single point of key management failure.

- Time-lock with reasonable latency, e.g., 48 hours, for awareness on privileged operations;
  AND
- 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 timelock contract and multi-signers addresses information with the public audience.

Long Term:

Timelock and DAO, the combination, *mitigate* by applying decentralization and transparency.

- Time-lock with reasonable latency, e.g., 48 hours, for awareness on privileged operations;
  AND
- Introduction of a DAO/governance/voting module to increase transparency and user involvement.
  AND
- A medium/blog link for sharing the timelock contract, multi-signers addresses, and DAO 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

[MEXAS, 05/11/2026]:

Ethereum Mainnet:

The MEXAS contract has transferred the ownership to a Gnosis Safe contract with 3/5 signers in the sensitive function signing process.

- Grant Role transaction hash for Gnosis Safe: https://etherscan.io/tx/0x12800fe905b49aca55d6ba5284f78ea57b18dc886899490c519943ba3e9efde6, Gnosis safe contract address: https://etherscan.io/address/0x82c40c2921dc724c36fa89d0d6014c6d3dfb7c08#code
- The 3/5 multisign addresses:
  1. EOA:0x26bD65AE120ed6a169Bb6cc5AAd2db23fb9d7D8F
  2. EOA:0x3e7Dd8dC8C9bf7Ea1139f626a4c62A8dd97eA15c
  3. EOA:0x1324CC2bB8Ac1dD809D7d1ECF87FE3387cfD2a9d
  4. EOA:0x9050401fd8e03dDB82df79Fc3A280feD7d360F71
  5. EOA:0x29d6206a6f3d4d74Edf0Ac36a9Fe0A3f8733cd25

Arbitrum Mainnet:

The MEXAS contract has transferred the ownership to a Gnosis Safe contract with 3/5 signers in the sensitive function signing process.

- Grant Role transaction hash for Gnosis Safe: https://arbiscan.io/tx/0x29d2871ebd1ce592de01e0419460c34846a8dbe85075fb68a2bc5adb2505de7b, Gnosis safe contract address: https://arbiscan.io/address/0x7851bB23D54Bc032A3eb82F4cCCCAD4287Ab62a4
- The 3/5 multisign addresses:
  1. EOA:0x26bD65AE120ed6a169Bb6cc5AAd2db23fb9d7D8F
  2. EOA:0x3e7Dd8dC8C9bf7Ea1139f626a4c62A8dd97eA15c
  3. EOA:0x1324CC2bB8Ac1dD809D7d1ECF87FE3387cfD2a9d
  4. EOA:0x9050401fd8e03dDB82df79Fc3A280feD7d360F71
  5. EOA:0x29d6206a6f3d4d74Edf0Ac36a9Fe0A3f8733cd25

Avalanche Mainnet:

The MEXAS contract has transferred the ownership to a Gnosis Safe contract with 3/5 signers in the sensitive function signing process.

- Grant Role transaction hash for Gnosis Safe: https://snowtrace.io/tx/0xf5efae3565afc48960273e1e1275da955415c9b7e07f113c077c2b62730980fe?chainid=43114, Gnosis safe contract address: https://snowtrace.io/address/0x524A6E0421D9bF2524d9f13595df1aefE2571A6A
- The 3/5 multisign addresses:
  1. EOA:0x26bD65AE120ed6a169Bb6cc5AAd2db23fb9d7D8F
  2. EOA:0x3e7Dd8dC8C9bf7Ea1139f626a4c62A8dd97eA15c

3. EOA:0x1324CC2bB8Ac1dD809D7d1ECF87FE3387cfD2a9d
4. EOA:0x9050401fd8e03dDB82df79Fc3A280feD7d360F71
5. EOA:0x29d6206a6f3d4d74Edf0Ac36a9Fe0A3f8733cd25

Base Mainnet:

The MEXAS contract has transferred the ownership to a Gnosis Safe contract with 3/5 signers in the sensitive function signing process.

- Grant Role transaction hash for Gnosis Safe: https://basescan.org/tx/0x94fc630393429abcb8924812099ec4f7ac3a55cef512ab8af2097b865ed2a0f7, Gnosis safe contract address: https://basescan.org/address/0x72c41E6A7F83dB2557092814299Ea5129111Cf75
- The 3/5 multisign addresses:
  1. EOA:0x26bD65AE120ed6a169Bb6cc5AAd2db23fb9d7D8F
  2. EOA:0x3e7Dd8dC8C9bf7Ea1139f626a4c62A8dd97eA15c
  3. EOA:0x1324CC2bB8Ac1dD809D7d1ECF87FE3387cfD2a9d
  4. EOA:0x9050401fd8e03dDB82df79Fc3A280feD7d360F71
  5. EOA:0x29d6206a6f3d4d74Edf0Ac36a9Fe0A3f8733cd25

BSC Mainnet:

The MEXAS contract has transferred the ownership to a Gnosis Safe contract with 3/5 signers in the sensitive function signing process.

- Grant Role transaction hash for Gnosis Safe: https://bscscan.com/tx/0xe63a3de6373767ea4dea5cdc1f0237b75c9ad8f2d5665d2c0c9bb7d399e75af4, Gnosis safe contract address: https://bscscan.com/address/0x42b8A305F548FA47Dd2309BC54198fcA0C9A15eA#code
- The 3/5 multisign addresses:
  1. EOA:0x26bD65AE120ed6a169Bb6cc5AAd2db23fb9d7D8F
  2. EOA:0x3e7Dd8dC8C9bf7Ea1139f626a4c62A8dd97eA15c
  3. EOA:0x1324CC2bB8Ac1dD809D7d1ECF87FE3387cfD2a9d
  4. EOA:0x9050401fd8e03dDB82df79Fc3A280feD7d360F71
  5. EOA:0x29d6206a6f3d4d74Edf0Ac36a9Fe0A3f8733cd25

[CertiK, 05/12/2026]: While this strategy has indeed reduced the risk, it's crucial to note that it has not completely eliminated it. CertiK strongly encourages the project team to periodically revisit the private key security management of all above-listed addresses.

MEX-04 | Local Variable Shadowing

Category	Severity	Location	Status
Coding Style	Minor	contracts/MEXAS.sol: 143	Acknowledged

Description

A local variable is shadowing another component defined elsewhere. This means that when the contract accesses the variable by its name, it will use the one defined locally, not the one defined in the other place. The use of the variable may lead to unexpected results and unintended behavior.

```
143     address owner,
```

- Local variable `owner` in `MEXAS.permit` shadows the function `owner` in `OwnableUpgradeable`.

Recommendation

It is recommended to remove or rename the local variable that shadows another definition to prevent potential issues and maintain the expected behavior of the smart contract.

Alleviation

[MEXAS, 05/11/2026]: The team acknowledged the issue and decided not to implement the recommended change in the current engagement.

APPENDIX | MEXAS

Finding Categories

Categories	Description
Centralization	Centralization findings detail the design choices of designating privileged roles or other centralized controls over the code.
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.

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.

Elevate Your Web3 Journey

CertiK is the largest Web3 security platform combining formal verification with audits and comprehensive security solutions.