CERTIK

Security Assessment

Venus - ACM Commands Aggregator

CertiK Assessed on Oct 7th, 2024

CertiK Assessed on Oct 7th, 2024

Venus - ACM Commands Aggregator

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

Executive Summary

TYPES	ECOSYSTEM	METHODS
Governance	Ethereum (ETH)	Manual Review, Static Analysis
LANGUAGE	**TIMELINE**	**KEY COMPONENTS**
Solidity	Delivered on 10/07/2024	N/A

CODEBASE
https://github.com/VenusProtocol/governance-contracts
View All in Codebase Page

COMMITS
Base: 92ad829e14c9883496146893b7ac0764b7208e48
Update1: 7ee75af4c6a04ee9a12643411d7f21b6166052fc
View All in Codebase Page

Vulnerability Summary

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

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.
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 Resolved	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 | VENUS - ACM COMMANDS AGGREGATOR

CODEBASE | VENUS - ACM COMMANDS AGGREGATOR

Repository

https://github.com/VenusProtocol/governance-contracts

Commit

Base: 92ad829e14c9883496146893b7ac0764b7208e48
Update1: 7ee75af4c6a04ee9a12643411d7f21b6166052fc

AUDIT SCOPE | VENUS - ACM COMMANDS AGGREGATOR

1 file audited • 1 file without findings

ID	Repo	File	SHA256 Checksum
ACM	VenusProtocol/governance-contracts	ACMCommandsAggregator.sol	4ef1c0ec4c578fd33c5cc9b0c832c33bc1deaa79b0d0af2f2557b81abcff7874

APPROACH & METHODS

VENUS - ACM COMMANDS AGGREGATOR

This report has been prepared for Venus to discover issues and vulnerabilities in the source code of the Venus - ACM Commands Aggregator 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.

SUMMARY | VENUS - ACM COMMANDS AGGREGATOR

This audit concerns the changes made in the in scope files in following PR:

https://github.com/VenusProtocol/governance-contracts/pull/90

Note that any centralization risks present in the existing codebase before this PR were not considered in this audit. We recommend all users to carefully review the centralization risks, much of which can be found in our previous audits which can be found here: https://skynet.certik.com/projects/venus.

In particular, this PR is designed to provide a permissionless contract that can be used for granting and revoking permissions in batches for the Access Control Manager contract across remote chains (non-BNB chains).

FINDINGS | VENUS - ACM COMMANDS AGGREGATOR

4	0	0	0	1	3
Total Findings	Critical	Major	Medium	Minor	Informational

This report has been prepared to discover issues and vulnerabilities for Venus - ACM Commands Aggregator. Through this audit, we have uncovered 4 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
ACM-02	Missing Zero Address Validation	Volatile Code	Minor	Resolved
ACM-01	Discussion On Sequence Of Granting, Executing, And Revoking Actions	Access Control	Informational	Acknowledged
ACM-03	Missing Natspec Comment For Contract	Inconsistency	Informational	Resolved
GLOBAL-01	Discussion On Current Addresses With `DEFAULT_ADMIN_ROLE`	Inconsistency	Informational	Resolved

ACM-02 | MISSING ZERO ADDRESS VALIDATION

Category	Severity	Location	Status
Volatile Code	Minor	ACMCommandsAggregator.sol (Base): 70	Resolved

Description

In the constructor, the input `_acm` is not checked to ensure it is not the zero address.

Recommendation

We recommend adding a check to ensure that the input `_acm` is not `address(0)`.

Alleviation

`[CertiK, 10/03/2024]`: The client made changes resolving the finding in commit b9070b009c7ed29454cf6ee9a2774fe17d023dd6.

ACM-01 | DISCUSSION ON SEQUENCE OF GRANTING, EXECUTING, AND REVOKING ACTIONS

Category	Severity	Location	Status
Access Control	Informational	ACMCommandsAggregator.sol (Base): 6~7	Acknowledged

Description

Venus describes the intended use of this contract with their AccessControlManager as follows:

1. Preload permissions to be granted or revoked in the `AccessControlManager`.
2. Make a VIP on BNB Chain for three commands executed on the corresponding remote network. The three commands are:
    - Grant the `DEFAULT_ADMIN_ROLE` in the `AccessControlManager` to the `ACMCommandsAggregator`.
    - Execute functions `executeGrantPermissions()` or `executeRevokePermissions()` with chosen preloaded permission id as needed to grant or revoke the preloaded permissions within the `AccessControlManager`.
    - Revoke `DEFAULT_ADMIN_ROLE` from the `ACMCommandsAggregator`.

The sequence of commands done in step 2 must be performed atomically within the same transaction. Otherwise, the protocol stands the risk of anyone granting or revoking permissions within the `AccessControlManager` within any of the remote chains. This is because all functions within the `ACMCommandsAggregator` are left permissionless.

In addition, the permissions associated with the `index` provided must be carefully reviewed prior to the execution of the VIP to ensure that the proper permissions are granted/revoked. In particular, it should be ensured that the `index` is not referencing permissions that were added by unintended entities.

Recommendation

Please confirm that the actions of granting `DEFAULT_ADMIN_ROLE`, executing granting or revoking permissions, and revoking `DEFAULT_ADMIN_ROLE` from `ACMCommandsAggregator` will be done atomically through VIPs.

Furthermore, we recommend clearly documenting the required structure of VIPs when interacting with this contract to ensure that the `DEFAULT_ADMIN_ROLE` is properly handled and that the `ACMCommandsAggregator` is not accidentally left with the `DEFAULT_ADMIN_ROLE`. Note that `executeGrantPermissions()` and `executeRevokePermissions()` could renounce the `DEFAULT_ADMIN_ROLE` after they grant or revoke permissions to help prevent such a scenario. However, this would then cause issues if permissions are desired to be granted and revoked for multiple ids, which may not align with your intended design.

Alleviation

`[Venus, 9/30/2024]` : "The second described step will be performed in the scope of a VIP, and therefore in a single transaction. We'll prepare VIP simulations, as usual, asking for several reviews before sharing the commands with the Venus community for the vote. We trust in that process to avoid any misconfiguration on the ACMCommandsAggregator, that could allow anyone to grant or revoke permissions."

ACM-03 | MISSING NATSPEC COMMENT FOR CONTRACT

Category	Severity	Location	Status
Inconsistency	Informational	ACMCommandsAggregator.sol (Base): 6	Resolved

Description

Other files within the codebase include NatSpec comments for the title, author, and summary of the contract. However, `ACMCommandsAggregator` does not have such comments.

Recommendation

We recommend adding NatSpec comments for the title, author, and summary of the contract to be consistent.

Alleviation

`[CertiK, 10/03/2024]`: The client made changes resolving the finding in commit 93280bfa9c997103144ed6d67644b852bfcfbdaa.

GLOBAL-01 | DISCUSSION ON CURRENT ADDRESSES WITH `DEFAULT_ADMIN_ROLE`

Category	Severity	Location	Status
Inconsistency	Informational		Resolved

Description

The documentation provided state the following:

"Normal Timelock contracts on each remote network will have the DEFAULT_ROLE in the AccessControlManager contract. So only Normal VIP's on BNB Chain (that will use the Normal Timelocks on the remote networks) will be able to complete the proposed plan, because no other timelock contract will be able to grant and revoke the DEFAULT_ROLE to/from the ACMCommandsAggregator."

However, when reviewing the `AccessControlManager` contracts deployed on the remote networks, we noticed that in addition to the normal timelock having the `DEFAULT_ADMIN_ROLE` (if it is deployed), a multi-sign is also given the `DEFAULT_ADMIN_ROLE`. This allows for the `DEFAULT_ADMIN_ROLE` to granted and revoked to/from the ACMCommandsAggregator through a method other than normal VIPs.

For example on Ethereum, the `AccessControlManager` contract is at address 0x230058da2D23eb8836EC5DB7037ef7250c56E25E and the mutli-sign at address 0x285960C5B22fD66A736C7136967A3eB15e93CC67 has the `DEFAULT_ADMIN_ROLE` along with the normal timelock at address 0xd969E79406c35E80750aAae061D402Aab9325714.

Can you please confirm if the intention is to revoke the `DEFAULT_ADMIN_ROLE` from the multi-signs and when this action will take place.

Recommendation

We recommend confirming whether the intention is to revoke the `DEFAULT_ADMIN_ROLE` from the multi-signs and providing information on when this action will take place.

Alleviation

`[Venus, 09/30/2024]`: "The DEFAULT_ADMIN_ROLE will be revoked from the guardian wallets (multisig wallets) that currently have that role. That is part of the plan to fully enable multichain governance. We even have the Pull Request open with the commands to be executed to do that:

https://github.com/VenusProtocol/vips/pull/364"

APPENDIX | VENUS - ACM COMMANDS AGGREGATOR

Finding Categories

Categories	Description
Access Control	Access Control findings are about security vulnerabilities that make protected assets unsafe.
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.

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.