VIBRANIUM AUDITS

Security Assessment

Serenity Shield

Verified by Vibranium Audits on 17 December 2023

Vibranium Audits Verified on December 17th, 2023

Serenity Shield

The security assessment was prepared by Vibranium Audits.

Executive Summary

TYPES	ECOSYSTEM	METHODS
DEFI	Ethereum/EVM	Manual Review, penetration testing and Static Analysis
LANGUAGE	**TIMELINE**	**KEY COMPONENTS**
Solidity	Delivered on 17/12/2023	N/A

CODEBASE

https://github.com/serenityshield/migration-vesting-contract

COMMITS

047df64dc7b8946178eb0326598c61b337e62132

Vulnerability Summary

6	0	0	0	6	0	0
Total Findings	Resolved	Mitigated	Partially Resolved	Acknowledged	Declined	Unresolved

0	Critical		Critical vulnerabilities are usually straightforward to exploit and can lead to the loss of user funds or contract state manipulation by external or internal actors.
0	High	0 Resolved	High vulnerabilities are usually harder to exploit, requiring specific conditions, or have a more limited scope, but can still lead to the loss of user funds or contract state manipulation by external or internal actors.
1	Medium	0 Resolved	Medium vulnerabilities are usually limited to state manipulations, but cannot lead to assets loss. Major deviations from best practices are also in this category.
2	Low	0 Resolved	Low vulnerabilities are related to outdated and unused code or minor gas optimization. These issues won't have a significant impact on code execution, but affect the code quality.
3	Informational	0 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.

TABLE OF CONTENTS | SERENITY SHIELD

CODEBASE | SERENITY SHIELD

Repository

https://github.com/serenityshield/migration-vesting-contract

Commits

047df64dc7b8946178eb0326598c61b337e62132

AUDIT SCOPE | SERENITY SHIELD

2 files audited ● 2 file with Acknowledged findings ● 0 files with Resolved findings

ID	Files	Commit Hash
● VVA	sersh-vesting.sol	047df64dc7b8946178eb0326598c61b337e62132
● EVA	sersh-vesting-escrow.sol	047df64dc7b8946178eb0326598c61b337e62132

APPROACH & METHODS | SERENITY SHIELD

This report has been prepared for SERENITY SHIELD(2023) to discover issues and vulnerabilities in the source code of the SERENITY SHIELD 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, rigorous Penetration Testing and Static Analysis techniques.

The auditing process pays special attention to the following considerations:

- Pen-Testing the smart contracts against both common and uncommon attack vectors.
- Assessing the code base 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 code base 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.
- Review unit tests to cover the possible use cases.
- Review functions for readability, especially for future development work.

FINDINGS | SERENITY SHIELD

6	0	1	2	3
Total Findings	High	Medium	Low	Informational

This report has been prepared to discover issues and vulnerabilities for SERENITY SHIELD. Through this audit, we have uncovered 11 issues ranging from different severity levels. Utilizing the techniques of Manual Review, Penetration Testing & Static Analysis to complement rigorous manual code reviews, we discovered the following findings:

ID	Title	Category	Severity	Status
VVA-01	Lack Of Emergency withdrawal	Logical Issue	Medium	Acknowledged
VVA-02 EVA-01	Central Contract Ownership	Logical Issue	Minor	Acknowledged
EVA-02	Unnecessary use of uint64	Logical Issue	Informational	Acknowledged
EVA-03 VVA-03	Error-Handling Optmizations	Logical Issue	Minor	Acknowledged
EVA-04	Presence of Unused Function	Logical Issue	Informational	Acknowledged
EVA-05 VVA-04	Lack of Documentation	Coding Style	Informational	Acknowledged

EVA-01 | Lack Of Emergency Withdrawal

Category	Severity	Location	Status
Logical Issue	Medium	sersh-vesting.sol	Acknowledged

Description

The smart contract **'sersh-vesting.sol' has functionalitites responsible for transfering tokens into the contract address and then withdrawing them under certain circumstances**. It is advised to implement and emergencyWithdraw() Function that allows the owner/admin to retrieve/withdraw the smart contract's balance of tokens in case of an emergency.

Recommendation

The implemented emergencyWithdraw() Function should not be overpowered by the 'notPaused' Modifier.

Example:

```
function emergencyWithdraw() external onlyOwner {
    uint256 balance = IERC20(vestingToken).balanceOf(address(this));
    bool success = IERC20(vestingToken).safeTransfer(owner(), balance);

    emit Witdhrawn();
}
```

VVA-02 WVA-01 | Central Contract Ownership

Categor y	Severity	Location	Status
Logical Issue	Minor	sersh-vesting.sol sersh-vesting-escrow.sol	Acknowledged

Description

Both contracts rely on an ownership system from OpenZeppelin's 'Ownable' Smart contract. With core functionalities dependent on the 'onlyOwner' modifier.
This could be problematic and potentially detrimental in the extreme case that the owner address is lost or in any other way compromised.

Recommendation

Consider implementing a more advanced system for access to these core functionalities, for example an Admin Access system where 2-3 addresses will have Admin Status is perfect for this use case.

EVA-02 | Unnecessary use of uint64

Categor y	Severity	Location	Status
Logical Issue	Informational	sersh-vesting-escrow.sol	Acknowledged

Description

Contract ‘sersh-vesting-escrow.sol’ uses uint64 for the variable _unvestingStep to track the progress of unvesting steps. There is no particular reason to use uint64, if this was done for gas optimizations, it is not fulfilling that goal .

Recommended

This point will have nothing to do with the safety or functionality of the smart contract, therefore adjusting the variable to uint256 or keeping it as uint64 will make no difference.

EVA-03 VVA-03 | Error-Handling Optmizations

Category	Severity	Location	Status
Logical Issue	Informational	sersh-vesting.sol sersh-vesting-escrow.sol	Acknowledged

Description

Some core functionalities, like 'canDeployVestingContract', contain multiple if statements that return an error message in case certain conditions aren't met.
Due to the number of these statements and the length of the error messages, it will be the source of highly augmented gas fees, and potentially blocking the execution of the transaction in cases of Network congestion due to Gas Limit exceeding.

Recommended

We Recommend the use of custom errors instead of the full length error messages to save up on gas usage; example:

```
error undefinedAddress();
...
if (buyer == address(0)) {
        revert undefinedAddress();
}
...
```

EVA-04 | Presence of Unused Function

Categor y	Severity	Location	Status
Logical Issue	Informational	sersh-vesting.sol	Acknowledged

Description

Contract ‘sersh-vesting.sol’ contains the function ‘triggerUnvestedEvent(...)’, which serves the only purpose of emitting the ‘unvested’ event, which isn’t called by any other functionality and doesn’t seem to serve any direct functionality.
Therefore it should be removed avoiding code redundancy.

EVA-05 VVA-04 | Lack of documentation

Categor y	Severity	Location	Status
Logical Issue	Informational	RentalWorkflow.sol WorkflowBase.sol	Acknowledged

Description

Althought the SERENITY SHIELD contracts set features some documentation on the main contract (sersh-vesting & sersh-vesting-escrow), it is recommended to fully document all the written code for better future communication between developers, auditors and any other involved party.

DISCLAIMER | VIBRANIUM AUDITS

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 Vibranium Audits 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 Vibranium Audits 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 Vibranium Audits position is that each company and individual are responsible for their own due diligence and continuous security Vibranium Audits 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 Vibranium Audits 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 VIBRANIUM AUDITS HEREBY DISCLAIMS ALL WARRANTIES WHETHER EXPRESS IMPLIED STATUTORY OR OTHERWISE WITH RESPECT TO THE SERVICES ASSESSMENT REPORT OR OTHER MATERIALS WITHOUT LIMITING THE FOREGOING VIBRANIUM AUDITS 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 VIBRANIUM AUDITS 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 ANOTHER 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 FORGOING, VIBRANIUM AUDITS PROVIDES NO WARRANTY OR UNDERTAKING, AND MAKES NO REPRESENTATION OF ANY KINDTHAT 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 VIBRANIUM AUDITS NOR ANY OF VIBRANIUM AUDITS AGENTS MAKES ANY REPRESENTATION OR WARRANTY OF ANY KIND EXPRESS OR IMPLIED AS TO THE ACCURACY RELIABILITY ORCURRENCY OF ANY INFORMATION OR CONTENT PROVIDED THROUGH THE SERVICE VIBRANIUM AUDITS 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 OWNEROR DISTRIBUTOR OF THE THIRD-PARTY MATERIALS

THE SERVICES ASSESSMENT REPORT AND ANY OTHER MATERIALS HERE UNDER 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 VIBRANIUM AUDITS 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 VIBRANIUM AUDITS WITH RESPECT TO SUCH SERVICES ASSESSMENT REPORT AND ANY ACCOMPANYING MATERIALS

THE REPRESENTATIONS AND WARRANTIES OF VIBRANIUM AUDITS 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 VIBRANIUM AUDITS 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 ORMATERIALS SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.

Vibranium | Securing the Web3 World

Vibranium Audits is a blockchain security company that was founded in 2021 by professors from the University of Greenwich and cyber-security engineers from ITI Capital. As pioneers in the field, Vibranium Audits utilizes best-in-class Formal Verification and AI technology to secure and monitor blockchains, smart contracts, and Web3 apps.