EtherAuthority

www.EtherAuthority.io
audit@etherauthority.io

SMART CONTRACT

Security Audit Report

Project:	MadViking Staking
Website:	madvikingstudios.com
Platform:	BNB Smart Chain
Language:	Solidity
Date:	April 1st, 2023

Table of contents

Introduction 4

Project Background 4

Audit Scope 5

Claimed Smart Contract Features 6

Audit Summary 7

Technical Quick Stats 8

Code Quality 9

Documentation 9

Use of Dependencies 9

AS-IS overview 10

Severity Definitions 11

Audit Findings 12

Conclusion 15

Our Methodology 16

Disclaimers 18

Appendix

- Code Flow Diagram 19
- Slither Results Log 20
- Solidity static analysis 21
- Solhint Linter 23

`

THIS IS SECURITY AUDIT REPORT DOCUMENT AND WHICH MAY CONTAIN INFORMATION WHICH IS CONFIDENTIAL. WHICH INCLUDES ANY POTENTIAL VULNERABILITIES AND MALICIOUS CODES WHICH CAN BE USED TO EXPLOIT THE SOFTWARE. THIS MUST BE REFERRED INTERNALLY AND ONLY SHOULD BE MADE AVAILABLE TO THE PUBLIC AFTER ISSUES ARE RESOLVED.

Introduction

EtherAuthority was contracted by the MadViking Staking system team to perform the Security audit of the MadViking Staking smart contract code. The audit has been performed using manual analysis as well as using automated software tools. This report presents all the findings regarding the audit performed on April 1st, 2023.

The purpose of this audit was to address the following:

- Ensure that all claimed functions exist and function correctly.
- Identify any security vulnerabilities that may be present in the smart contract.

Project Background

- MadViking staking is a staking system with reward distribution.
- Stakers can stake with MVG tokens.
- Stakers will get GEMS tokens as rewards as per the tokens they stake and the token unit set by the owner.

Audit scope

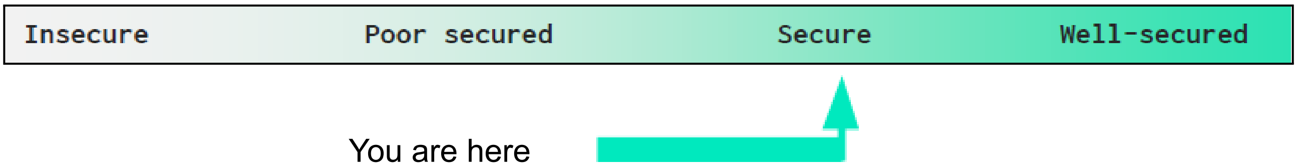
Name	**Code Review and Security Analysis Report for Mad Viking Staking system Smart Contract**
Platform	**BSC / Solidity**
File	MadVikingStaking.sol
File MD5 Hash	ECDA31F1D3666237D299C88C592C62E8
Audit Date	April 1st, 2023

Claimed Smart Contract Features

Claimed Feature Detail	Our Observation
Tokenomics: ● Rewards unit: 1 GEMS ● Token unit: 0.1 Million ● Time Unit: 1 day ● Open Zeppelin standard code is used.	**YES, This is valid.**
<u>Owner Specifications:</u> ● Token unit value can be changed by the admin. ● The time unit value can be changed by the admin. ● Admin can change the pause state of the staking system. ● The reward unit value can be changed by the admin.	**YES, This is valid.**

Audit Summary

According to the standard audit assessment, Customer`s solidity smart contracts are **"Secured"**. Also, these contracts do contain owner control, which does not make them fully decentralized.



We used various tools like Slither, Solhint and Remix IDE. At the same time this finding is based on critical analysis of the manual audit.

All issues found during automated analysis were manually reviewed and applicable vulnerabilities are presented in the Audit overview section. General overview is presented in AS-IS section and all identified issues can be found in the Audit overview section.

We found 0 critical, 0 high, 1 medium and 0 low and some very low level issues.

Investors Advice: Technical audit of the smart contract does not guarantee the ethical nature of the project. Any owner controlled functions should be executed by the owner with responsibility. All investors/users are advised to do their due diligence before investing in the project.

Technical Quick Stats

Main Category	Subcategory	Result
Contract Programming	Solidity version not specified	Passed
	Solidity version too old	Passed
	Integer overflow/underflow	Passed
	Function input parameters lack of check	Moderate
	Function input parameters check bypass	Passed
	Function access control lacks management	Passed
	Critical operation lacks event log	Passed
	Human/contract checks bypass	Passed
	Random number generation/use vulnerability	N/A
	Fallback function misuse	Passed
	Race condition	Passed
	Logical vulnerability	Passed
	Features claimed	Passed
	Other programming issues	Passed
Code Specification	Function visibility not explicitly declared	Passed
	Var. storage location not explicitly declared	Passed
	Use keywords/functions to be deprecated	Passed
	Unused code	Passed
Gas Optimization	“Out of Gas” Issue	Passed
	High consumption ‘for/while’ loop	Passed
	High consumption ‘storage’ storage	Passed
	Assert() misuse	Passed
Business Risk	The maximum limit for mintage not set	Passed
	“Short Address” Attack	Passed
	“Double Spend” Attack	Passed

Overall Audit Result: **PASSED**

Code Quality

This audit scope has 1 smart contract. Smart contract contains Libraries, Smart contracts, inherits and Interfaces. This is a compact and well written smart contract.

The libraries in the MadViking Staking system are part of its logical algorithm. A library is a different type of smart contract that contains reusable code. Once deployed on the blockchain (only once), it is assigned a specific address and its properties / methods can be reused many times by other contracts in the MadViking Staking system .

The MadViking Staking system team has not provided scenario and unit test scripts, which would have helped to determine the integrity of the code in an automated way.

Code parts are well commented on in the smart contracts. Ethereum's NatSpec commenting style is used, which is a good thing.

Documentation

We were given a MadViking Staking system smart contract code in the form of a file. The hash of that code is mentioned above in the table.

As mentioned above, code parts are **well** commented. And the logic is straightforward. So it is easy to quickly understand the programming flow as well as complex code logic. Comments are very helpful in understanding the overall architecture of the protocol.

Another source of information was its official website: https://madvikingstudios.com which provided rich information about the project architecture and tokenomics.

Use of Dependencies

As per our observation, the libraries are used in this smart contract infrastructure that are based on well known industry standard open source projects.

Apart from libraries, its functions are not used in external smart contract calls.

AS-IS overview

Functions

Sl.	Functions	Type	Observation	Conclusion
1	constructor	write	Immutable variables	Refer to audit findings
2	nonReentrant	modifier	Passed	No Issue
3	_nonReentrantBefore	write	Passed	No Issue
4	_nonReentrantAfter	write	Passed	No Issue
5	_reentrancyGuardEntered	internal	Passed	No Issue
6	supportsInterface	read	Passed	No Issue
7	getRoleMember	read	Passed	No Issue
8	getRoleMemberCount	read	Passed	No Issue
9	_grantRole	internal	Passed	No Issue
10	_revokeRole	internal	Passed	No Issue
11	requireAdmin	modifier	Passed	No Issue
12	systemActive	modifier	Passed	No Issue
13	stakerInfo	read	Passed	No Issue
14	setSystemPaused	write	requiring admin	No Issue
15	setRewardUnit	write	Unit limit is not set	Refer to audit findings
16	setTokenUnit	write	Unit limit is not set	Refer to audit findings
17	setTimeunit	write	Unit limit is not set	Refer to audit findings
18	calculateClaimableReward	read	Passed	No Issue
19	stake	write	Passed	No Issue
20	unstake	write	Passed	No Issue
21	claim	write	Passed	No Issue
22	_calculateNewRewards	internal	Passed	No Issue
23	_claim	internal	system Active	No Issue
24	_stake	internal	Passed	No Issue
25	_unstake	internal	Passed	No Issue

Severity Definitions

Risk Level	Description
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to token loss etc.
High	High-level vulnerabilities are difficult to exploit; however, they also have significant impact on smart contract execution, e.g. public access to crucial
Medium	Medium-level vulnerabilities are important to fix; however, they can't lead to tokens lose
Low	Low-level vulnerabilities are mostly related to outdated, unused etc. code snippets, that can't have significant impact on execution
Lowest / Code Style / Best Practice	Lowest-level vulnerabilities, code style violations and info statements can't affect smart contract execution and can be ignored.

Audit Findings

Critical Severity

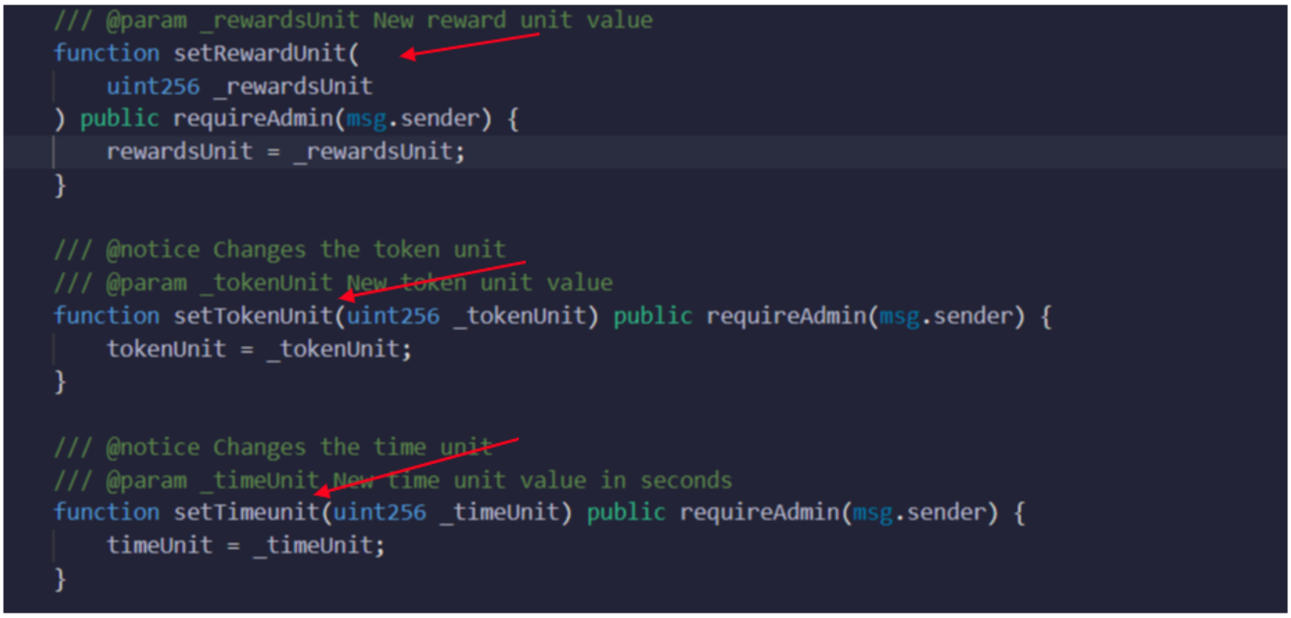
No Critical severity vulnerabilities were found.

High Severity

No High severity vulnerabilities were found.

Medium

(1) Unit limit is not set:



```
/// @param _rewardsUnit New reward unit value
function setRewardUnit(
    uint256 _rewardsUnit
) public requireAdmin(msg.sender) {
    rewardsUnit = _rewardsUnit;
}

/// @notice Changes the token unit
/// @param _tokenUnit New token unit value
function setTokenUnit(uint256 _tokenUnit) public requireAdmin(msg.sender) {
    tokenUnit = _tokenUnit;
}

/// @notice Changes the time unit
/// @param _timeUnit New time unit value in seconds
function setTimeunit(uint256 _timeUnit) public requireAdmin(msg.sender) {
    timeUnit = _timeUnit;
}
```

In setRewardUnit , setTokenUnit , setTimeunit functions, Admin can set the individual unit to any variable. This might deter investors as they could be wary that these units might one day be set to 100%.

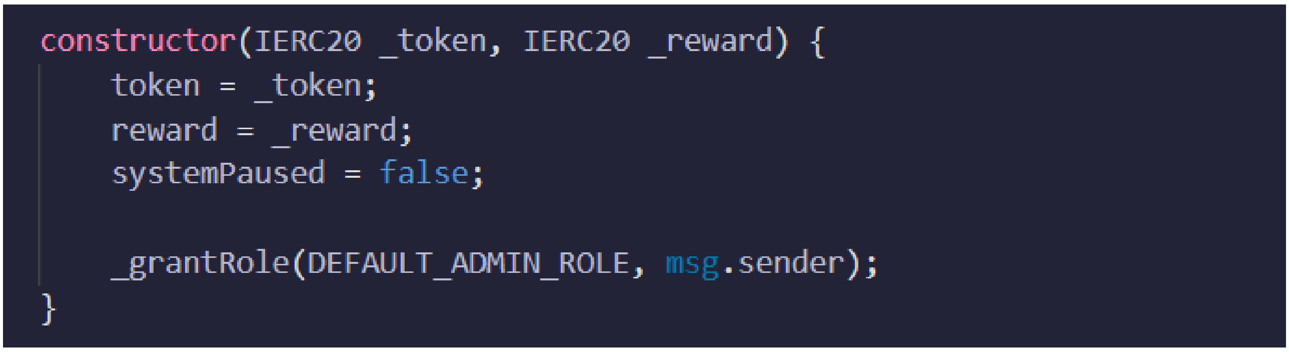
Resolution: Consider adding an explicit cap to the units on every unit adjustment function.

Low

No Low severity vulnerabilities were found.

Very Low / Informational / Best practices:

(1) Immutable variables:



```
constructor(IERC20 _token, IERC20 _reward) {
    token = _token;
    reward = _reward;
    systemPaused = false;

    _grantRole(DEFAULT_ADMIN_ROLE, msg.sender);
}
```

The token and reward are set only in the constructor function.

Resolution: We suggest declaring them as immutable variables.

Centralization

This smart contract has some functions which can be executed by the Admin (Owner) only. If the admin wallet private key would be compromised, then it would create trouble. Following are Admin functions:

MadVikingStaking.sol

- setTokenUnit: Token unit value can be changed by the admin.
- setTimeunit: The time unit value can be changed by the admin.
- setSystemPaused: Admin can change the pause state of the staking system.
- setRewardUnit: The reward unit value can be changed by the admin.

To make the smart contract 100% decentralized, we suggest renouncing ownership in the smart contract once its function is completed.

Conclusion

We were given a contract code in the form of a file and we have used all possible tests based on given objects. We have observed 1 medium severity issue and 1 Informational severity issue in the code. but those are not critical ones. So, **it's good to go for the mainnet deployment**.

Since possible test cases can be unlimited for such smart contracts protocol, we provide no such guarantee of future outcomes. We have used all the latest static tools and manual observations to cover maximum possible test cases to scan everything.

Smart contracts within the scope were manually reviewed and analyzed with static analysis tools. Smart Contract's high-level description of functionality was presented in the As-is overview section of the report.

The audit report contains all found security vulnerabilities and other issues in the reviewed code.

The security state of the reviewed smart contract, based on standard audit procedure scope, is **"Secured".**

Our Methodology

We like to work with a transparent process and make our reviews a collaborative effort. The goals of our security audits are to improve the quality of systems we review and aim for sufficient remediation to help protect users. The following is the methodology we use in our security audit process.

Manual Code Review:

In manually reviewing all of the code, we look for any potential issues with code logic, error handling, protocol and header parsing, cryptographic errors, and random number generators. We also watch for areas where more defensive programming could reduce the risk of future mistakes and speed up future audits. Although our primary focus is on the in-scope code, we examine dependency code and behavior when it is relevant to a particular line of investigation.

Vulnerability Analysis:

Our audit techniques included manual code analysis, user interface interaction, and whitebox penetration testing. We look at the project's web site to get a high level understanding of what functionality the software under review provides. We then meet with the developers to gain an appreciation of their vision of the software. We install and use the relevant software, exploring the user interactions and roles. While we do this, we brainstorm threat models and attack surfaces. We read design documentation, review other audit results, search for similar projects, examine source code dependencies, skim open issue tickets, and generally investigate details other than the implementation.

Documenting Results:

We follow a conservative, transparent process for analyzing potential security vulnerabilities and seeing them through successful remediation. Whenever a potential issue is discovered, we immediately create an Issue entry for it in this document, even though we have not yet verified the feasibility and impact of the issue. This process is conservative because we document our suspicions early even if they are later shown to not represent exploitable vulnerabilities. We generally follow a process of first documenting the suspicion with unresolved questions, then confirming the issue through code analysis, live experimentation, or automated tests. Code analysis is the most tentative, and we strive to provide test code, log captures, or screenshots demonstrating our confirmation. After this we analyze the feasibility of an attack in a live system.

Suggested Solutions:

We search for immediate mitigations that live deployments can take, and finally we suggest the requirements for remediation engineering for future releases. The mitigation and remediation recommendations should be scrutinized by the developers and deployment engineers, and successful mitigation and remediation is an ongoing collaborative process after we deliver our report, and before the details are made public.

Disclaimers

EtherAuthority.io Disclaimer

EtherAuthority team has analyzed this smart contract in accordance with the best industry practices at the date of this report, in relation to: cybersecurity vulnerabilities and issues in smart contract source code, the details of which are disclosed in this report, (Source Code); the Source Code compilation, deployment and functionality (performing the intended functions).

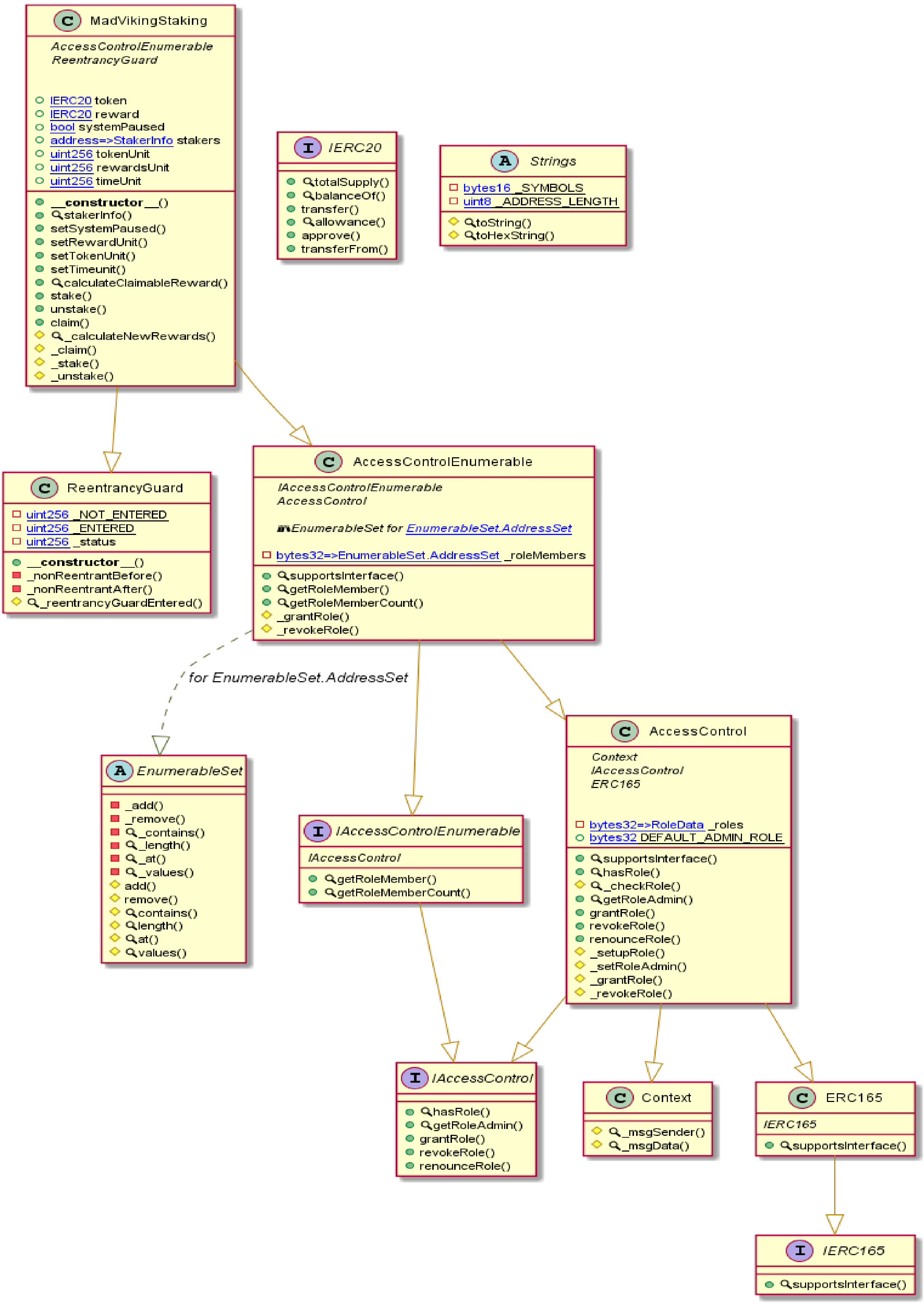
Due to the fact that the total number of test cases are unlimited, the audit makes no statements or warranties on security of the code. It also cannot be considered as a sufficient assessment regarding the utility and safety of the code, bugfree status or any other statements of the contract. While we have done our best in conducting the analysis and producing this report, it is important to note that you should not rely on this report only. We also suggest conducting a bug bounty program to confirm the high level of security of this smart contract.

Technical Disclaimer

Smart contracts are deployed and executed on the blockchain platform. The platform, its programming language, and other software related to the smart contract can have their own vulnerabilities that can lead to hacks. Thus, the audit can’t guarantee explicit security of the audited smart contracts.

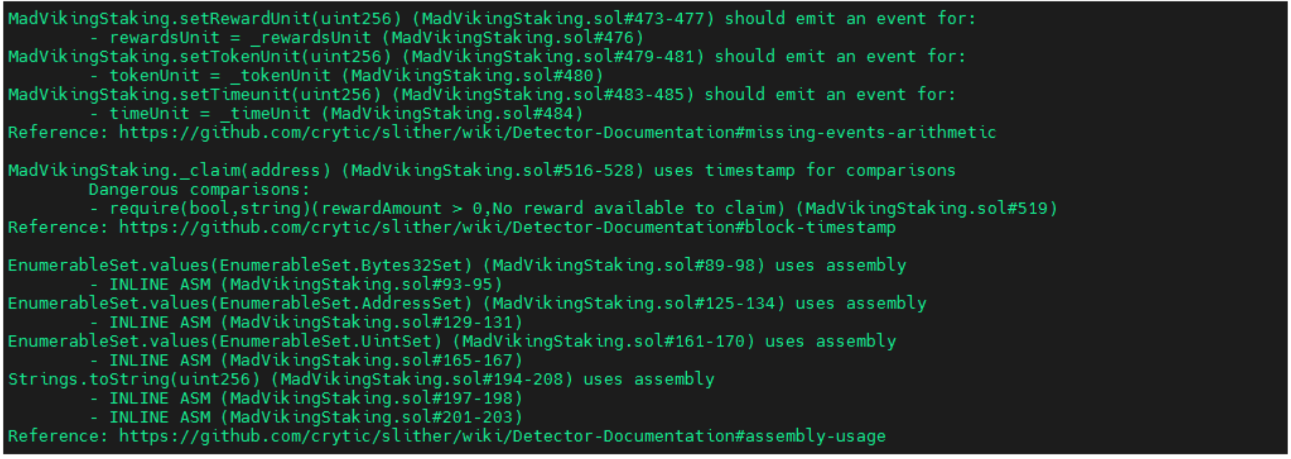
Appendix

Code Flow Diagram - MadViking Staking System

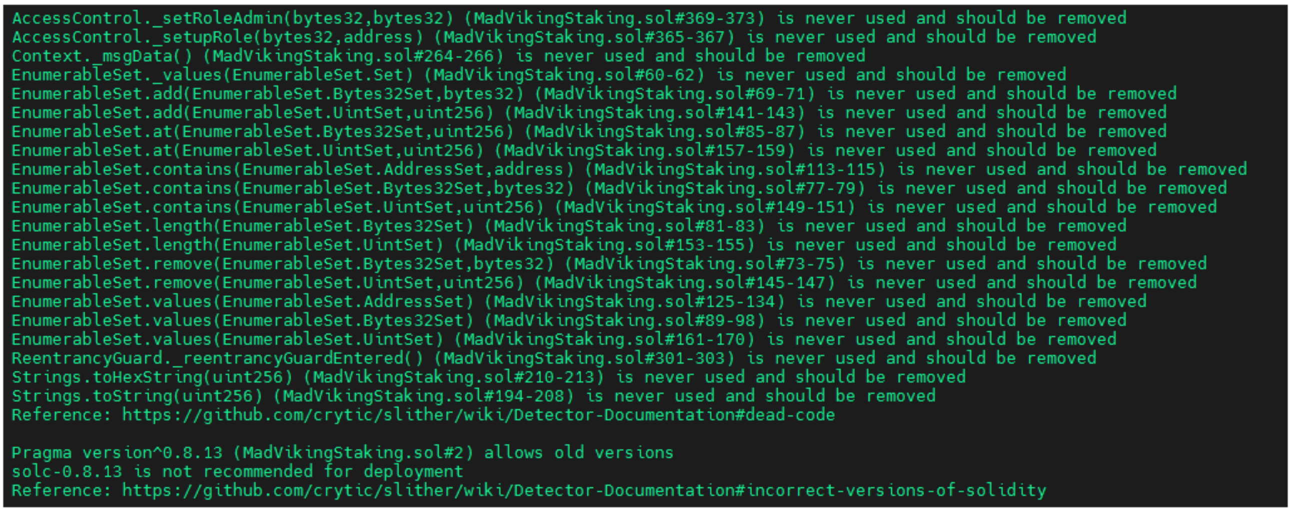


Slither Results Log

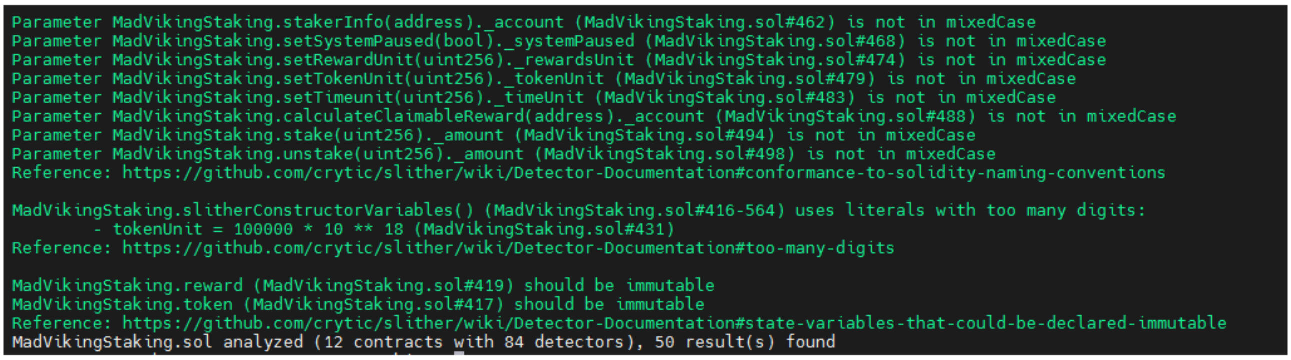
Slither Log >> MadVikingStaking.sol



```
MadVikingStaking.setRewardUnit(uint256) (MadVikingStaking.sol#473-477) should emit an event for:
        - rewardsUnit = _rewardsUnit (MadVikingStaking.sol#476)
MadVikingStaking.setTokenUnit(uint256) (MadVikingStaking.sol#479-481) should emit an event for:
        - tokenUnit = _tokenUnit (MadVikingStaking.sol#480)
MadVikingStaking.setTimeunit(uint256) (MadVikingStaking.sol#483-485) should emit an event for:
        - timeUnit = _timeUnit (MadVikingStaking.sol#484)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#missing-events-arithmetic

MadVikingStaking._claim(address) (MadVikingStaking.sol#516-528) uses timestamp for comparisons
        Dangerous comparisons:
        - require(bool,string)(rewardAmount > 0,No reward available to claim) (MadVikingStaking.sol#519)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#block-timestamp

EnumerableSet.values(EnumerableSet.Bytes32Set) (MadVikingStaking.sol#89-98) uses assembly
        - INLINE ASM (MadVikingStaking.sol#93-95)
EnumerableSet.values(EnumerableSet.AddressSet) (MadVikingStaking.sol#125-134) uses assembly
        - INLINE ASM (MadVikingStaking.sol#129-131)
EnumerableSet.values(EnumerableSet.UintSet) (MadVikingStaking.sol#161-170) uses assembly
        - INLINE ASM (MadVikingStaking.sol#165-167)
Strings.toString(uint256) (MadVikingStaking.sol#194-208) uses assembly
        - INLINE ASM (MadVikingStaking.sol#197-198)
        - INLINE ASM (MadVikingStaking.sol#201-203)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#assembly-usage
```



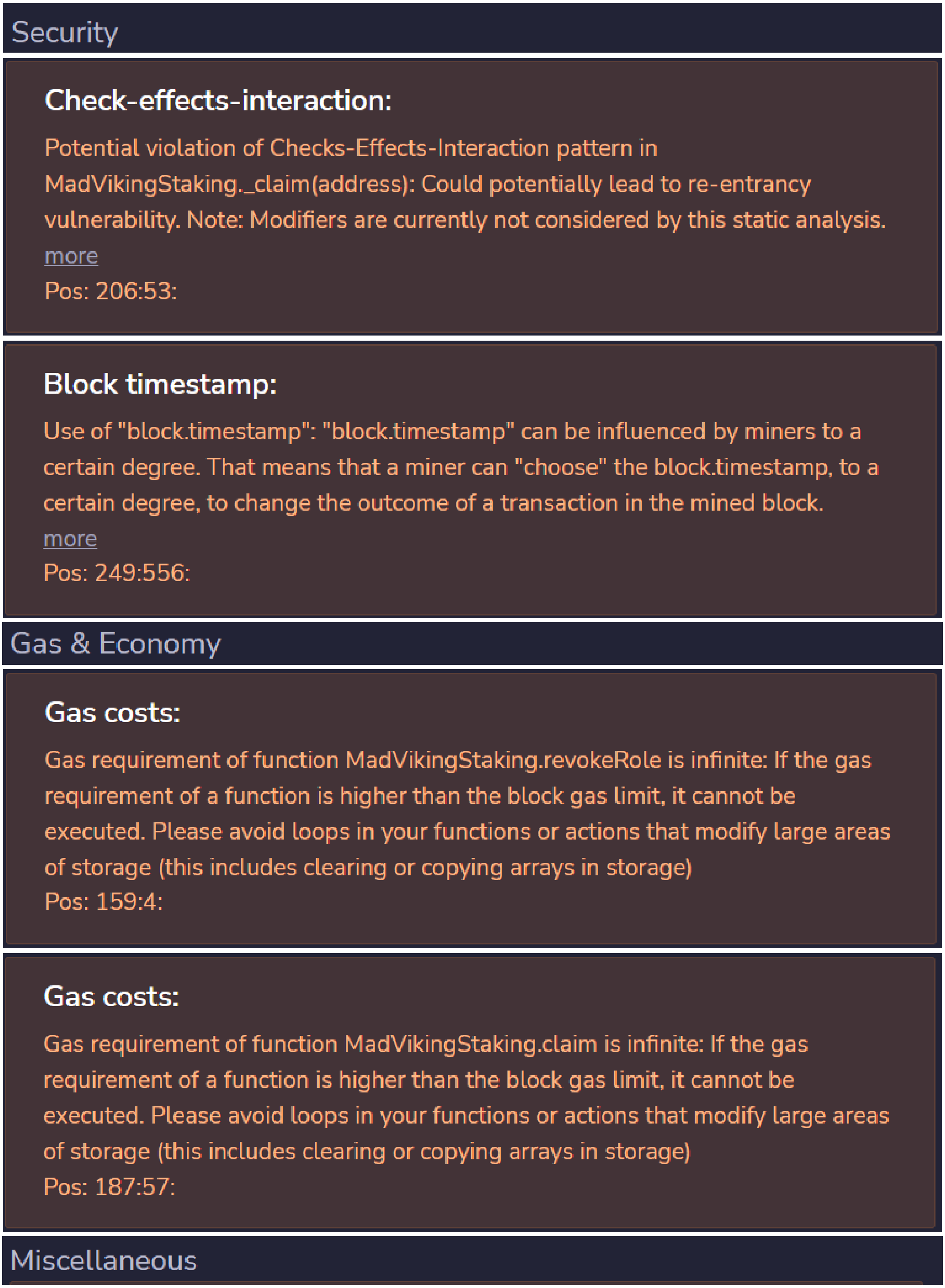
```
AccessControl._setRoleAdmin(bytes32,bytes32) (MadVikingStaking.sol#369-373) is never used and should be removed
AccessControl._setupRole(bytes32,address) (MadVikingStaking.sol#365-367) is never used and should be removed
Context._msgData() (MadVikingStaking.sol#264-266) is never used and should be removed
EnumerableSet._values(EnumerableSet.Set) (MadVikingStaking.sol#60-62) is never used and should be removed
EnumerableSet.add(EnumerableSet.Bytes32Set,bytes32) (MadVikingStaking.sol#69-71) is never used and should be removed
EnumerableSet.add(EnumerableSet.UintSet,uint256) (MadVikingStaking.sol#141-143) is never used and should be removed
EnumerableSet.at(EnumerableSet.Bytes32Set,uint256) (MadVikingStaking.sol#85-87) is never used and should be removed
EnumerableSet.at(EnumerableSet.UintSet,uint256) (MadVikingStaking.sol#157-159) is never used and should be removed
EnumerableSet.contains(EnumerableSet.AddressSet,address) (MadVikingStaking.sol#113-115) is never used and should be removed
EnumerableSet.contains(EnumerableSet.Bytes32Set,bytes32) (MadVikingStaking.sol#77-79) is never used and should be removed
EnumerableSet.contains(EnumerableSet.UintSet,uint256) (MadVikingStaking.sol#149-151) is never used and should be removed
EnumerableSet.length(EnumerableSet.Bytes32Set) (MadVikingStaking.sol#81-83) is never used and should be removed
EnumerableSet.length(EnumerableSet.UintSet) (MadVikingStaking.sol#153-155) is never used and should be removed
EnumerableSet.remove(EnumerableSet.Bytes32Set,bytes32) (MadVikingStaking.sol#73-75) is never used and should be removed
EnumerableSet.remove(EnumerableSet.UintSet,uint256) (MadVikingStaking.sol#145-147) is never used and should be removed
EnumerableSet.values(EnumerableSet.AddressSet) (MadVikingStaking.sol#125-134) is never used and should be removed
EnumerableSet.values(EnumerableSet.Bytes32Set) (MadVikingStaking.sol#89-98) is never used and should be removed
EnumerableSet.values(EnumerableSet.UintSet) (MadVikingStaking.sol#161-170) is never used and should be removed
ReentrancyGuard._reentrancyGuardEntered() (MadVikingStaking.sol#301-303) is never used and should be removed
Strings.toHexString(uint256) (MadVikingStaking.sol#210-213) is never used and should be removed
Strings.toString(uint256) (MadVikingStaking.sol#194-208) is never used and should be removed
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code

Pragma version^0.8.13 (MadVikingStaking.sol#2) allows old versions
solc-0.8.13 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity
```



```
Parameter MadVikingStaking.stakerInfo(address)._account (MadVikingStaking.sol#462) is not in mixedCase
Parameter MadVikingStaking.setSystemPaused(bool)._systemPaused (MadVikingStaking.sol#468) is not in mixedCase
Parameter MadVikingStaking.setRewardUnit(uint256)._rewardsUnit (MadVikingStaking.sol#474) is not in mixedCase
Parameter MadVikingStaking.setTokenUnit(uint256)._tokenUnit (MadVikingStaking.sol#479) is not in mixedCase
Parameter MadVikingStaking.setTimeunit(uint256)._timeUnit (MadVikingStaking.sol#483) is not in mixedCase
Parameter MadVikingStaking.calculateClaimableReward(address)._account (MadVikingStaking.sol#488) is not in mixedCase
Parameter MadVikingStaking.stake(uint256)._amount (MadVikingStaking.sol#494) is not in mixedCase
Parameter MadVikingStaking.unstake(uint256)._amount (MadVikingStaking.sol#498) is not in mixedCase
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions

MadVikingStaking.slitherConstructorVariables() (MadVikingStaking.sol#416-564) uses literals with too many digits:
        - tokenUnit = 100000 * 10 ** 18 (MadVikingStaking.sol#431)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#too-many-digits

MadVikingStaking.reward (MadVikingStaking.sol#419) should be immutable
MadVikingStaking.token (MadVikingStaking.sol#417) should be immutable
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declared-immutable
MadVikingStaking.sol analyzed (12 contracts with 84 detectors), 50 result(s) found
```

Solidity Static Analysis

MadVikingStaking.sol



Security

Check-effects-interaction:

Potential violation of Checks-Effects-Interaction pattern in MadVikingStaking._claim(address): Could potentially lead to re-entrancy vulnerability. Note: Modifiers are currently not considered by this static analysis.
more
Pos: 206:53:

Block timestamp:

Use of "block.timestamp": "block.timestamp" can be influenced by miners to a certain degree. That means that a miner can "choose" the block.timestamp, to a certain degree, to change the outcome of a transaction in the mined block.
more
Pos: 249:556:

Gas & Economy

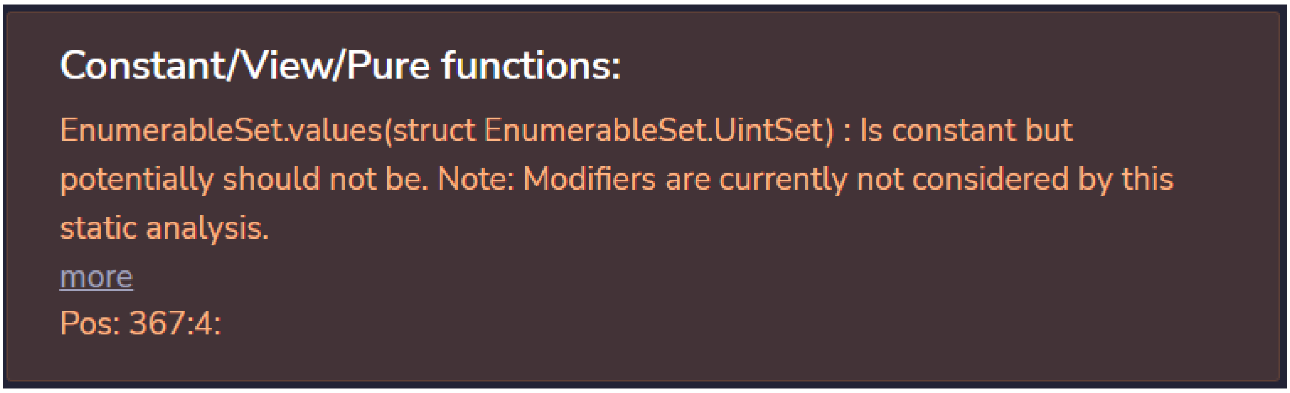
Gas costs:

Gas requirement of function MadVikingStaking.revokeRole is infinite: If the gas requirement of a function is higher than the block gas limit, it cannot be executed. Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage)
Pos: 159:4:

Gas costs:

Gas requirement of function MadVikingStaking.claim is infinite: If the gas requirement of a function is higher than the block gas limit, it cannot be executed. Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage)
Pos: 187:57:

Miscellaneous

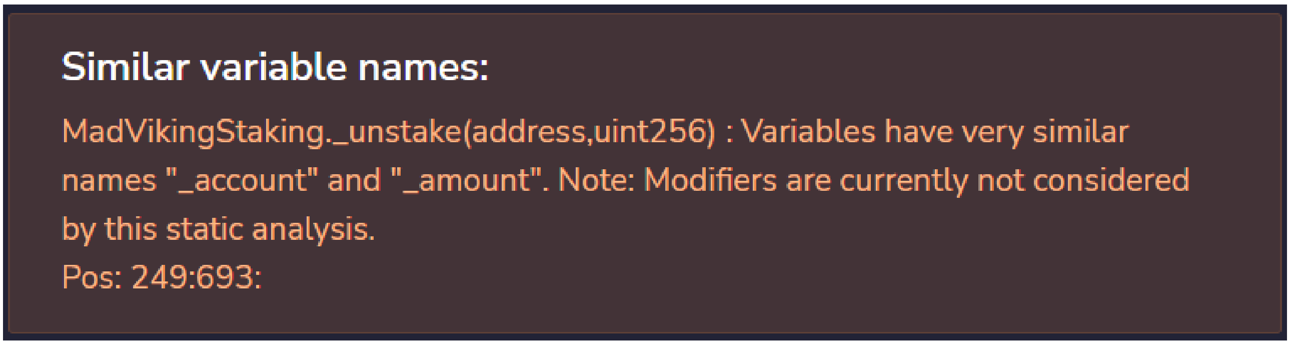


Constant/View/Pure functions:

EnumerableSet.values(struct EnumerableSet.UintSet) : Is constant but potentially should not be. Note: Modifiers are currently not considered by this static analysis.

more

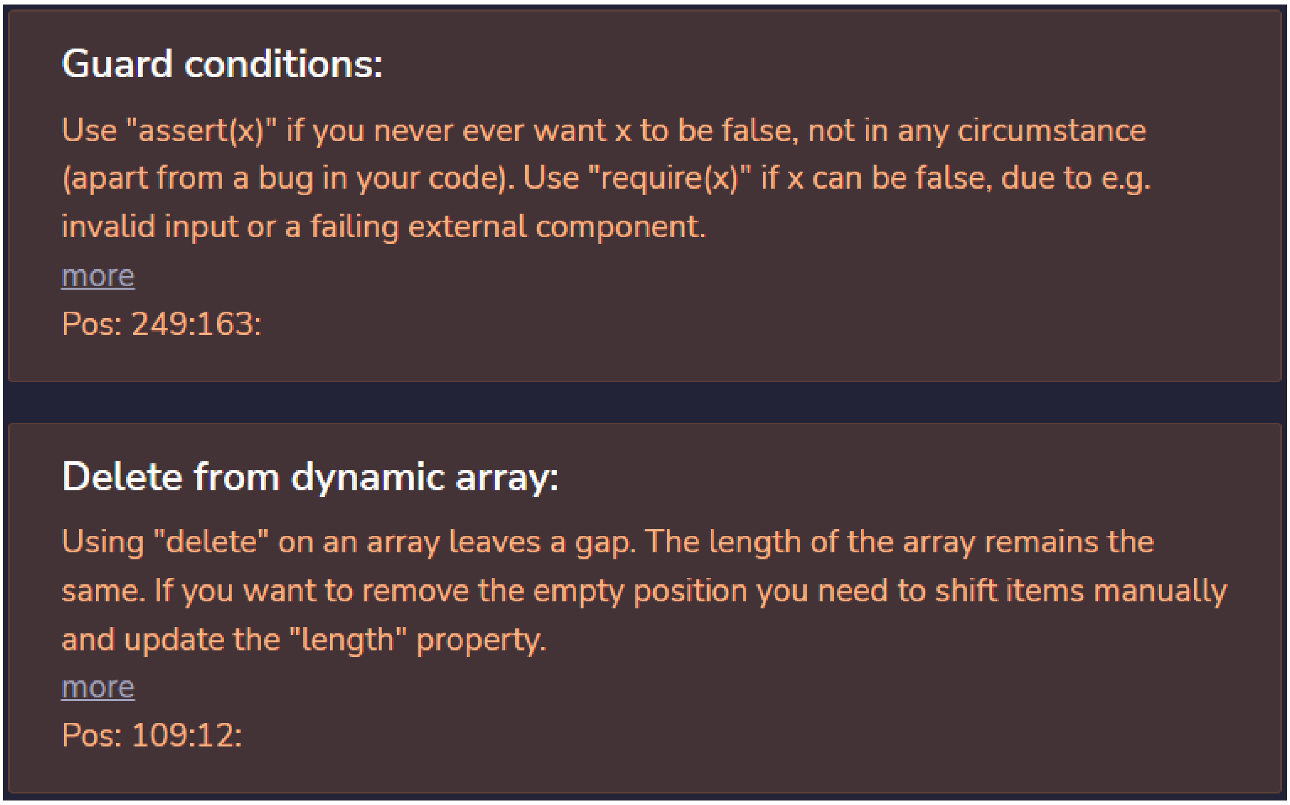
Pos: 367:4:



Similar variable names:

MadVikingStaking._unstake(address,uint256) : Variables have very similar names "_account" and "_amount". Note: Modifiers are currently not considered by this static analysis.

Pos: 249:693:



Guard conditions:

Use "assert(x)" if you never ever want x to be false, not in any circumstance (apart from a bug in your code). Use "require(x)" if x can be false, due to e.g. invalid input or a failing external component.

more

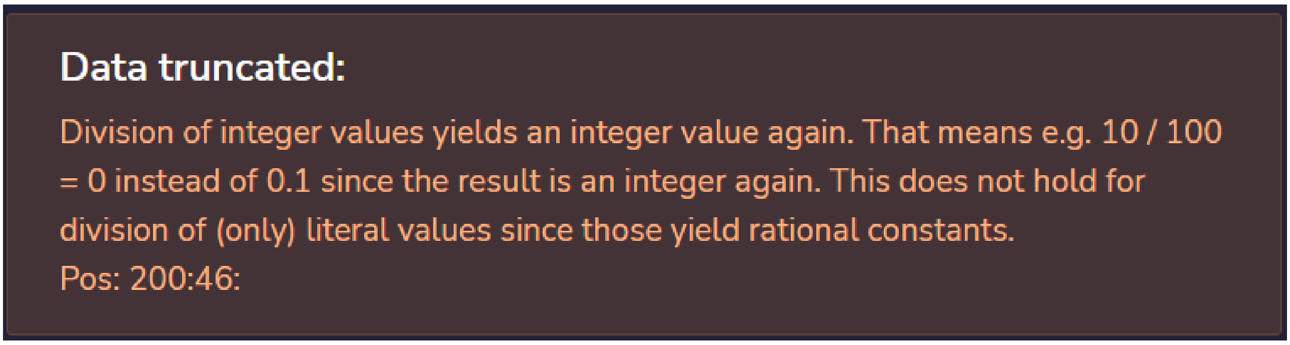
Pos: 249:163:

Delete from dynamic array:

Using "delete" on an array leaves a gap. The length of the array remains the same. If you want to remove the empty position you need to shift items manually and update the "length" property.

more

Pos: 109:12:



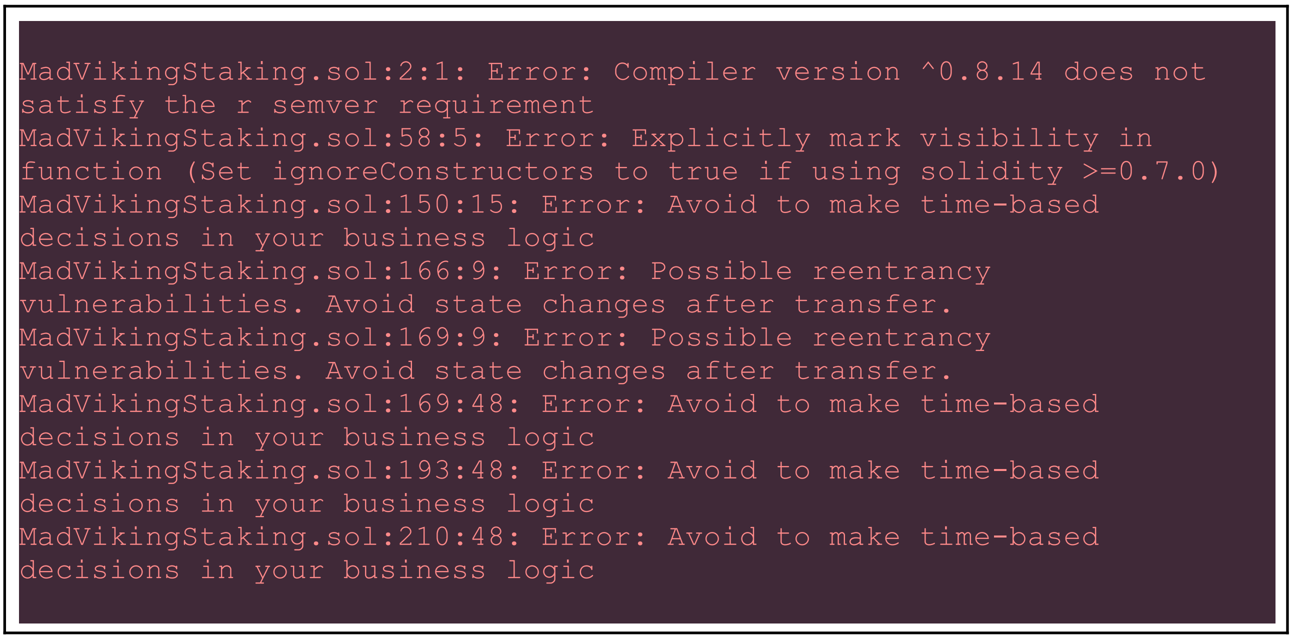
Data truncated:

Division of integer values yields an integer value again. That means e.g. 10 / 100 = 0 instead of 0.1 since the result is an integer again. This does not hold for division of (only) literal values since those yield rational constants.

Pos: 200:46:

Solhint Linter

MadVikingStaking.sol



```
MadVikingStaking.sol:2:1: Error: Compiler version ^0.8.14 does not
satisfy the r semver requirement
MadVikingStaking.sol:58:5: Error: Explicitly mark visibility in
function (Set ignoreConstructors to true if using solidity >=0.7.0)
MadVikingStaking.sol:150:15: Error: Avoid to make time-based
decisions in your business logic
MadVikingStaking.sol:166:9: Error: Possible reentrancy
vulnerabilities. Avoid state changes after transfer.
MadVikingStaking.sol:169:9: Error: Possible reentrancy
vulnerabilities. Avoid state changes after transfer.
MadVikingStaking.sol:169:48: Error: Avoid to make time-based
decisions in your business logic
MadVikingStaking.sol:193:48: Error: Avoid to make time-based
decisions in your business logic
MadVikingStaking.sol:210:48: Error: Avoid to make time-based
decisions in your business logic
```

Software analysis result:

These software reported many false positive results and some are informational issues. So, those issues can be safely ignored.

EtherAuthority

Email: audit@EtherAuthority.io