SOLIDProof

Bring trust into your projects

Blockchain Security | Smart Contract Audits | KYC Development | Marketing

MADE IN GERMANY

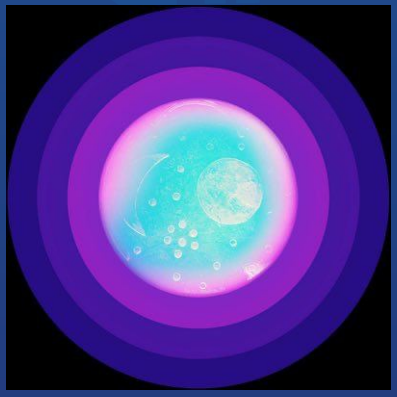
Dione Protocol

Audit

Security Assessment

29. March, 2023

For



Disclaimer

SolidProof.io reports are not, nor should be considered, an “endorsement” or “disapproval” of any particular project or team. These reports are not, nor should be considered, an indication of the economics or value of any “product” or “asset” created by any team. SolidProof.io do not cover testing or auditing the integration with external contract or services (such as Unicrypt, Uniswap, PancakeSwap etc’...)

SolidProof.io Audits do not provide any warranty or guarantee regarding the absolute bug- free nature of the technology analyzed, nor do they provide any indication of the technology proprietors. SolidProof Audits should not be used in any way to make decisions around investment or involvement with any particular project. These reports in no way provide investment advice, nor should be leveraged as investment advice of any sort.

SolidProof.io Reports represent an extensive auditing 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. SolidProof’s position is that each company and individual are responsible for their own due diligence and continuous security. SolidProof in no way claims any guarantee of security or functionality of the technology we agree to analyze.

Version	Date	Description
1.0	24. March 2023	• Layout project • Automated- /Manual-Security Testing • Summary
1.1	29. March 2023	• Reaudit

Network
Ethereum

Website
https://dioneprotocol.com

Telegram
t.me/DioneProtocol

Twitter
twitter.com/DioneProtocol

Instagram
instagram.com/DioneProtocol

YouTube
youtube.com/DioneProtocol

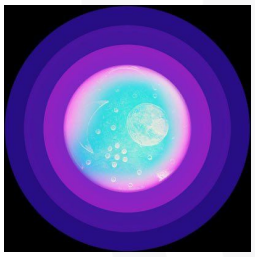
Description

This document, the Whitepaper, is the only source of truth regarding Dione. The technologies and products introduced in this document are currently in development and this document will continue to evolve. Therefore, this document does not aim to provide definite and absolute answers.

Project Engagement

During the Date of 21 March 2023, **Dione Protocol Team** engaged Solidproof.io to audit smart contracts that they created. The engagement was technical in nature and focused on identifying security flaws in the design and implementation of the contracts. They provided Solidproof.io with access to their code repository and whitepaper.

Logo



Contract Link

v1.0

- **DioneStaking (Proxy)**:
  https://etherscan.io/address/0xc7D446AE32791D96eF04983D5c9233348ae4bBAf

- **Implementation**: https://etherscan.io/address/0x04108C0B1E615aB7765383F35E4fAb8628760646#code

v1.1

- **DioneStaking (Proxy)**:
  https://etherscan.io/address/0xc7D446AE32791D96eF04983D5c9233348ae4bBAf

- **Implementation**: https://etherscan.io/address/0x0c6dFD9B2f0bB08e52BCc0C20fE4c4957Fb58f3E#code

Note for Investors: We only Audited a staking token contract for **Dione Protocol**. However, If the project has other contracts (for example, a Presale, or token contract etc), and they were not provided to us in the audit scope then we cannot comment on its security and we are not responsible for it in any way.

Vulnerability & Risk Level

Risk represents the probability that a certain source-threat will exploit vulnerability, and the impact of that event on the organization or system. Risk Level is computed based on CVSS version 3.0.

Level	Value	Vulnerability	Risk (Required Action)
Critical	9 - 10	A vulnerability that can disrupt the contract functioning in a number of scenarios, or creates a risk that the contract may be broken.	Immediate action to reduce risk level.
High	7 – 8.9	A vulnerability that affects the desired outcome when using a contract, or provides the opportunity to use a contract in an unintended way.	Implementation of corrective actions as soon aspossible.
Medium	4 – 6.9	A vulnerability that could affect the desired outcome of executing the contract in a specific scenario.	Implementation of corrective actions in a certain period.
Low	2 – 3.9	A vulnerability that does not have a significant impact on possible scenarios for the use of the contract and is probably subjective.	Implementation of certain corrective actions or accepting the risk.
Informational	0 – 1.9	A vulnerability that have informational character but is not effecting any of the code.	An observation that does not determine a level of risk

Auditing Strategy and Techniques Applied

Throughout the review process, care was taken to evaluate the repository for security-related issues, code quality, and adherence to specification and best practices. To do so, reviewed line-by-line by our team of expert pentesters and smart contract developers, documenting any issues as there were discovered.

Methodology

The auditing process follows a routine series of steps:

1. Code review that includes the following:
    i) Review of the specifications, sources, and instructions provided to SolidProof to make sure we understand the size, scope, and functionality of the smart contract.
    ii) Manual review of code, which is the process of reading source code line-by-line in an attempt to identify potential vulnerabilities.
    iii) Comparison to specification, which is the process of checking whether the code does what the specifications, sources, and instructions provided to SolidProof describe.

2. Testing and automated analysis that includes the following:
    i) Test coverage analysis, which is the process of determining whether the test cases are actually covering the code and how much code is exercised when we run those test cases.
    ii) Symbolic execution, which is analysing a program to determine what inputs causes each part of a program to execute.

3. Best practices review, which is a review of the smart contracts to improve efficiency, effectiveness, clarify, maintainability, security, and control based on the established industry and academic practices, recommendations, and research.

4. Specific, itemized, actionable recommendations to help you take steps to secure your smart contracts.

Used Code from other Frameworks/Smart Contracts (direct imports)

Imported packages:

```
@openzeppelin/contracts-upgradeable/utils/ContextUpgradeable.sol
@openzeppelin/contracts-upgradeable/access/OwnableUpgradeable.sol
@openzeppelin/contracts-upgradeable/math/SafeMathUpgradeable.sol
@openzeppelin/contracts-upgradeable/utils/ReentrancyGuardUpgradeable.sol
@openzeppelin/contracts-upgradeable/token/ERC20/SafeERC20Upgradeable.sol
@openzeppelin/contracts-upgradeable/proxy/Initializable.sol
@openzeppelin/contracts-upgradeable/utils/EnumerableSetUpgradeable.sol
./interfaces/IDione.sol
```

Tested Contract Files

This audit covered the following files listed below with a SHA-1 Hash.

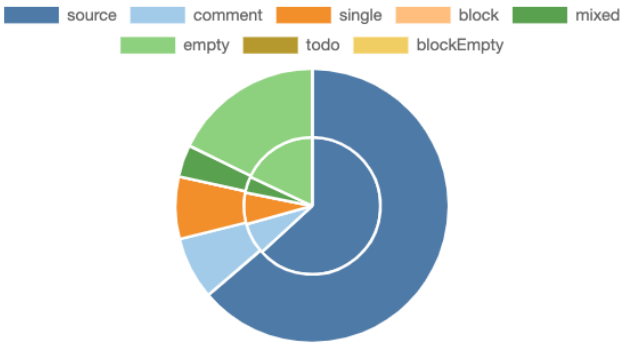
A file with a different Hash has been modified, intentionally or otherwise, after the security review. A different Hash could be (but not necessarily) an indication of a changed condition or potential vulnerability that was not within the scope of this review.

v1.0

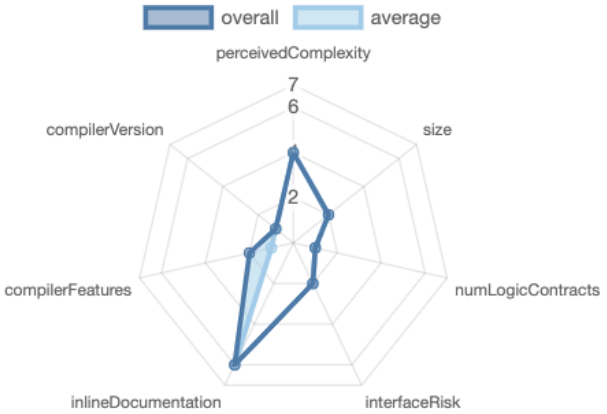
File Name	SHA-1 Hash
contracts/ DioneStaking.sol	796f3f2801aae304d95ed75610332ea6e60a0498

Metrics

Source Lines
v1.0



Risk Level
v1.0



Capabilities

Components

📝Contracts	📚Libraries	🔍Interfaces	💊Abstract
1	0	0	0

Exposed Functions

This section lists functions that are explicitly declared public or payable. Please note that getter methods for public stateVars are not included.

🌐Public	💰Payable
19	0

External	Internal	Private	Pure	View
17	32	0	0	9

StateVariables

Total	🌐Public
21	19

Capabilities

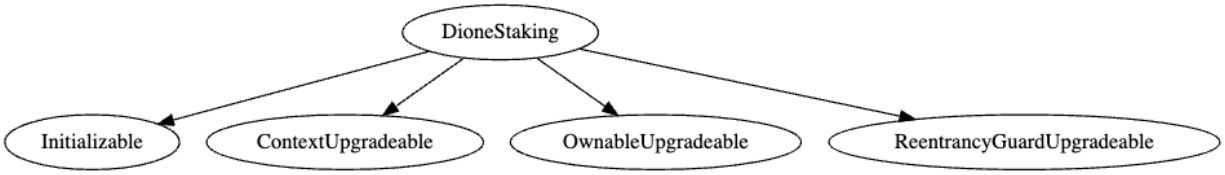
Solidity Versions observed	🧪 Experimental Features	💰 Can Receive Funds	🖥️ Uses Assembly	💣 Has Destroyable Contracts
`0.6.12`				

📩 Transfers ETH	⚡ Low-Level Calls	👥 DelegateCall	🧱 Uses Hash Functions	🪚 ECRecover	🌀 New/Create/Create2

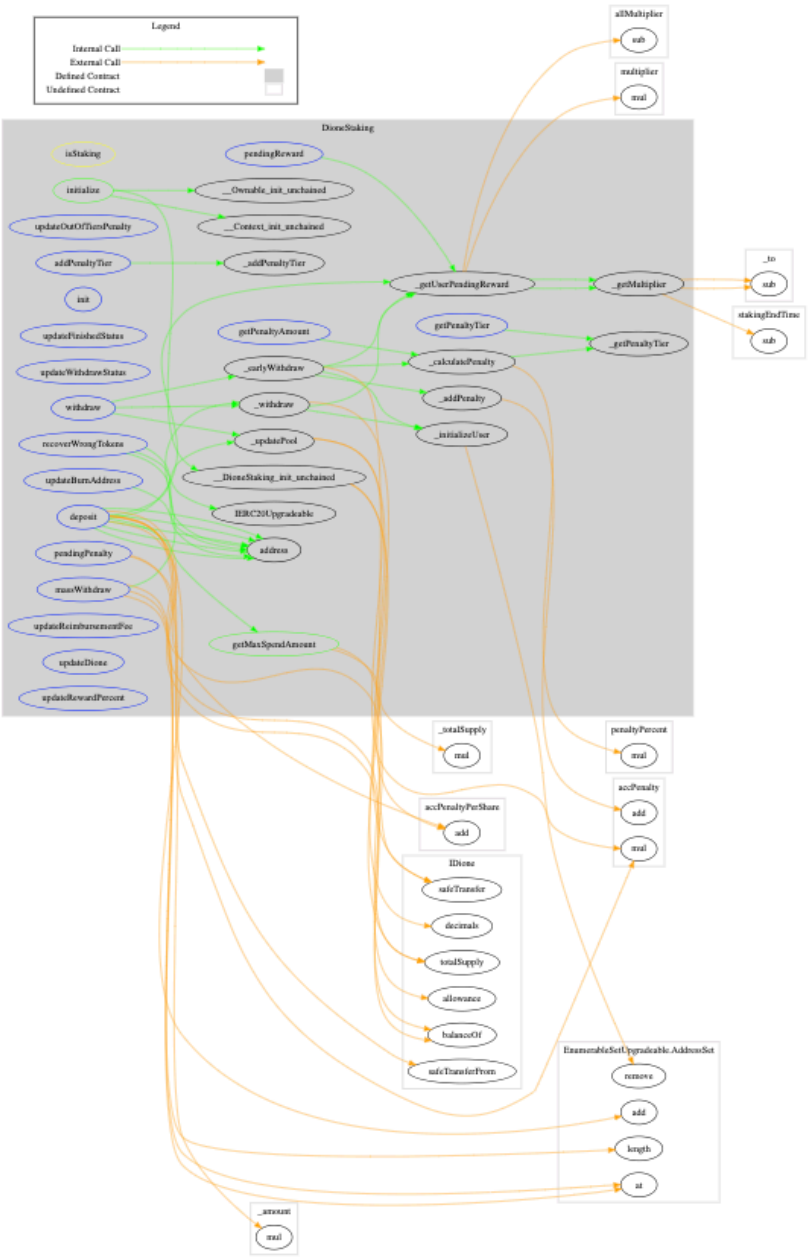
♻️ TryCatch	Σ Unchecked

Inheritance Graph

v1.0



CallGraph
v1.0



Scope of Work/Verify Claims

The above token Team provided us with the files that needs to be tested (Github, Bscscan, Etherscan, files, etc.). The scope of the audit is the main contract (usual the same name as team appended with .sol).

We will verify the following claims:

1. Is contract an upgradeable
2. Deployer cannot lock user funds
3. Deployer cannot pause the contract
4. Deployer cannot set fees
5. Overall checkup (Smart Contract Security)

Is contract an upgradeable

Name	
Is contract an upgradeable?	Yes

Comments:

v1.0

- Owner can deploy a new version of the contract which can change any limit and give owner new privileges
    - Be aware of this and do your own research for the contract which is the contract pointing to

Write functions of contract v1.0

1. addPenaltyTier (0xe916dc0c)
2. deposit (0xb6b55f25)
3. init (0xb7b0422d)
4. initialize (0xc350a1b5)
5. massWithdraw (0xbf0a196d)
6. recoverWrongTokens (0x3f138d4b)
7. renounceOwnership (0x715018a6)
8. transferOwnership (0xf2fde38b)
9. updateFinishedStatus (0x183fecf1)
10. updateOutOfTiersPenalty (0x678f43b5)
11. updateReimbursementFee (0x56157a3c)
12. updateRewardPercent (0x3ca45ae1)
13. updateWithdrawStatus (0xbd674692)
14. withdraw (0x3ccfd60b)

Deployer cannot lock user funds

Name	Exist	Tested	Status
Deployer can lock	✓	✓	✗

Comments:

v1.0

- Owner can lock user funds by disabling the withdraw function (which will force users to pay the penalty for early withdraw) and changing the staking token address, in which case the users won't be able to withdraw staked tokens.

Deployer cannot pause the contract

Name	Exist	Tested	Status
Deployer cannot pause	✓	✓	✓

Comments:

v1.0

- Owner cannot pause contract

Deployer cannot set fees

Name	Exist	Tested	Status
Deployer can set fees over 10%	✓	✓	✓
Deployer can set fees to nearly 100% or to 100%	✓	✓	✓

Comments:

v1.1

- Penalty cannot be set without any limitations. The maximum can be 10%

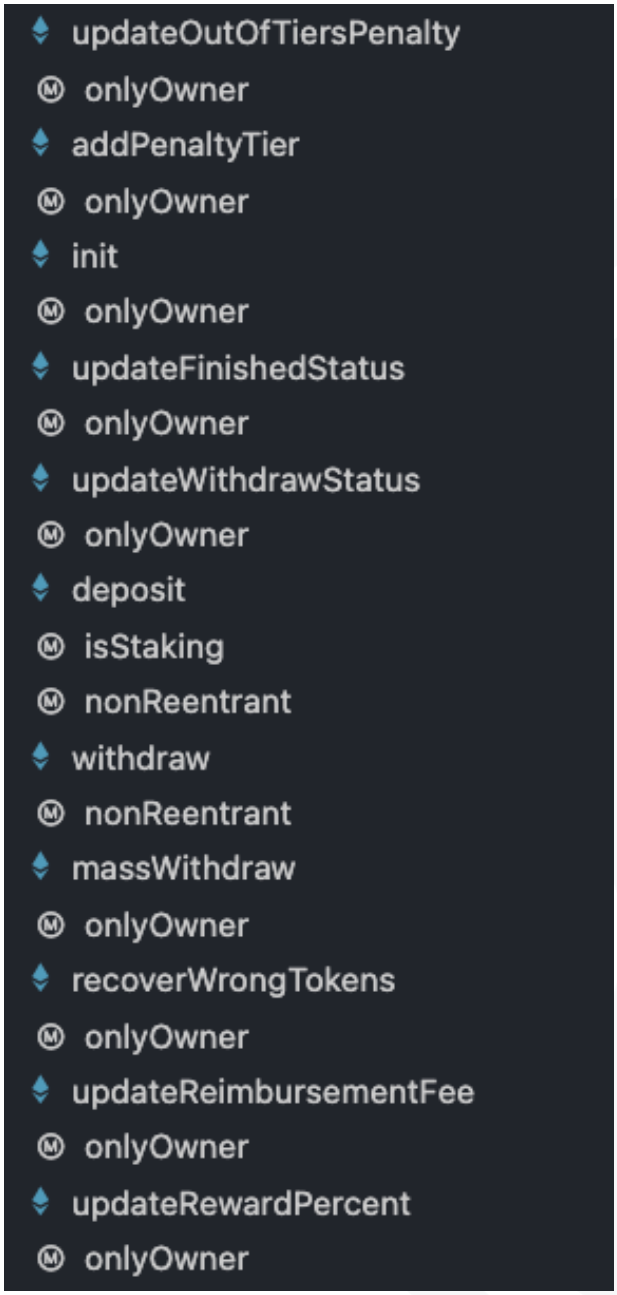
Overall checkup (Smart Contract Security)

Tested	Verified
✓	✓

Legend

Attribute	Symbol
Verified / Checked	✓
Partly Verified	⚑
Unverified / Not checked	✗
Not available	-

Modifiers and public functions
v1.1



Ownership Privileges

- The owner can update the out of tiers penalty percent to any arbitrary value.
- Add penalty tiers with any arbitrary value for validity
- Enable/Disable the finishing status of staking
- Withdraw tokens from the contract but not the staking tokens.
- Update reimbursement fee, and reward percent to any arbitrary value
- Please note that the owner can stop deposits at anytime by updating the "*isFinished*" status

Please check if an OnlyOwner or similar restrictive modifier has been forgotten.

Source Units in Scope
v1.0

File	Logic Contracts	Interfaces	Lines	nLines	nSLOC	Comment Lines	Complex. Score
contracts/DioneStaking.sol	1		474	466	347	41	271
Totals	**1**		**474**	**466**	**347**	**41**	**271**

Legend

Attribute	Description
Lines	total lines of the source unit
nLines	normalised lines of the source unit (e.g. normalises functions spanning multiple lines)
nSLOC	normalised source lines of code (only source-code lines; no comments, no blank lines)
Comment Lines	lines containing single or block comments
Complexity Score	a custom complexity score derived from code statements that are known to introduce code complexity (branches, loops, calls, external interfaces, ...)

Audit Results

Critical issues

No critical issues

High issues

No high issues

Medium issues

Issue	File	Type	Line	Description
#1	Main	Owner can drain tokens	300	The owner is able to withdraw staked tokens from the contract into the “BurnAddress” because the owner can set the Burn address to any wallet at the time of initialisation. Moreover, the withdraw function transfers the withdrawal amount to the burn address.
#2	Main	Impossible Withdraw	285	It is impossible to withdraw the staked tokens from the contract without paying the penalty because the withdraw function sends the staked amount to the burn address. Moreover, if a user choses to withdraw early then the staked tokens can be withdrawn but only by paying the penalty. The owner can also force the accounts to withdraw early and pay the penalty.

Low issues

No low issues

Informational issues

No informational issues

Alleviation

The medium issues stated above are acknowledged, and the **SolidProof** team received the following response from **Dione Protocol**'s Team on **29 March 2023, 10:24 a.m UTC**:

"Yes because we are going to be bridging the tokens to the new blockchain coin for the user.

The user will no longer be holding on to Dione token after they withdraw once they have fulfilled their staking term because we will be airdropping them the same amount in Dione coin to their wallets.

This is all in our disclosures to the stakers as well before they stake they have to sign off on terms of service.
For each burning, there is an event which will be emitted.

The bridge will listen to them and airdrop the migrated tokens in the dione blockchain to the users."

Audit Comments

We recommend you to use the special form of comments (NatSpec Format, Follow link for more information https://docs.soliditylang.org/en/latest/natspec-format.html) for your contracts to provide rich documentation for functions, return variables and more. This helps investors to make clear what that variables, functions etc. do.

29. March 2023:

- There is still an owner (Owner still has not renounced ownership)
- Owner can deploy a new version of the contract which can change any limit and give owner new privileges
- Read whole report and modifiers section for more information

SWC Attacks

ID	Title	Relationships	Status
SWC-136	Unencrypted Private Data On-Chain	CWE-767: Access to Critical Private Variable via Public Method	PASSED
SWC-135	Code With No Effects	CWE-1164: Irrelevant Code	PASSED
SWC-134	Message call with hardcoded gas amount	CWE-655: Improper Initialization	PASSED
SWC-133	Hash Collisions With Multiple Variable Length Arguments	CWE-294: Authentication Bypass by Capture-replay	PASSED
SWC-132	Unexpected Ether balance	CWE-667: Improper Locking	PASSED
SWC-131	Presence of unused variables	CWE-1164: Irrelevant Code	PASSED
SWC-130	Right-To-Left-Override control character (U+202E)	CWE-451: User Interface (UI) Misrepresentation of Critical Information	PASSED
SWC-129	Typographical Error	CWE-480: Use of Incorrect Operator	PASSED
SWC-128	DoS With Block Gas Limit	CWE-400: Uncontrolled Resource Consumption	PASSED

SWC-127	Arbitrary Jump with Function Type Variable	CWE-695: Use of Low-Level Functionality	PASSED
SWC-125	Incorrect Inheritance Order	CWE-696: Incorrect Behavior Order	PASSED
SWC-124	Write to Arbitrary Storage Location	CWE-123: Write-what-where Condition	PASSED
SWC-123	Requirement Violation	CWE-573: Improper Following of Specification by Caller	PASSED
SWC-122	Lack of Proper Signature Verification	CWE-345: Insufficient Verification of Data Authenticity	PASSED
SWC-121	Missing Protection against Signature Replay Attacks	CWE-347: Improper Verification of Cryptographic Signature	PASSED
SWC-120	Weak Sources of Randomness from Chain Attributes	CWE-330: Use of Insufficiently Random Values	PASSED
SWC-119	Shadowing State Variables	CWE-710: Improper Adherence to Coding Standards	PASSED
SWC-118	Incorrect Constructor Name	CWE-665: Improper Initialization	PASSED
SWC-117	Signature Malleability	CWE-347: Improper Verification of Cryptographic Signature	PASSED

SWC-116	Timestamp Dependence	CWE-829: Inclusion of Functionality from Untrusted Control Sphere	PASSED
SWC-115	Authorization through tx.origin	CWE-477: Use of Obsolete Function	PASSED
SWC-114	Transaction Order Dependence	CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	PASSED
SWC-113	DoS with Failed Call	CWE-703: Improper Check or Handling of Exceptional Conditions	PASSED
SWC-112	Delegatecall to Untrusted Callee	CWE-829: Inclusion of Functionality from Untrusted Control Sphere	PASSED
SWC-111	Use of Deprecated Solidity Functions	CWE-477: Use of Obsolete Function	PASSED
SWC-110	Assert Violation	CWE-670: Always-Incorrect Control Flow Implementation	PASSED
SWC-109	Uninitialized Storage Pointer	CWE-824: Access of Uninitialized Pointer	PASSED
SWC-108	State Variable Default Visibility	CWE-710: Improper Adherence to Coding Standards	PASSED
SWC-107	Reentrancy	CWE-841: Improper Enforcement of Behavioral Workflow	PASSED
SWC-106	Unprotected SELFDESTRUCT Instruction	CWE-284: Improper Access Control	PASSED

SWC-105	Unprotected Ether Withdrawal	CWE-284: Improper Access Control	PASSED
SWC-104	Unchecked Call Return Value	CWE-252: Unchecked Return Value	PASSED
SWC-103	Floating Pragma	CWE-664: Improper Control of a Resource Through its Lifetime	PASSED
SWC-102	Outdated Compiler Version	CWE-937: Using Components with Known Vulnerabilities	PASSED
SWC-101	Integer Overflow and Underflow	CWE-682: Incorrect Calculation	PASSED
SWC-100	Function Default Visibility	CWE-710: Improper Adherence to Coding Standards	PASSED