SOLIDProof

Bring trust into your projects

Blockchain Security | Smart Contract Audits | KYC Development | Marketing

MADE IN GERMANY

Deelit

AUDIT

SECURITY ASSESSMENT

24. October, 2024

FOR

DEELIT

Introduction

SolidProof.io is a brand of the officially registered company Future Visions Deutschland. We're mainly focused on Blockchain Security, such as Smart Contract Audits and KYC verification for project teams.
Solidproof.io assesses potential security issues in the smart contracts implementations, reviews for potential inconsistencies between the code base and the whitepaper/documentation, and provides suggestions for improvement.

Disclaimer

SolidProof.io reports are not, nor should they be considered, an "endorsement" or "disapproval" of any particular project or team. These reports are not, nor should they be considered, an indication of the economics or value of any "product" or "asset" created by any team. SolidProof.io does not cover testing or auditing the integration with external contracts 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 analysed, 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 the security or functionality of the technology we agree to analyse.

Project Overview

Summary

Project Name	Deelit
Website	https://deelit.net/en
About the project	The Deelit protocol is at the heart of what we call “secure payments” on the Deelit application. “Secure payment” is a payment system that secures transactions between two parties using blockchain technology. The major contribution of this system is to enable an exchange without intermediaries with the possibility of conflict resolution if and only if one of the parties requests it.
Chain	BASE
Language	Solidity
Codebase Link	AccessManagerProxy: https://basescan.org/address/0x52c38502192CF9657B0053C49e9C78F188D6C77D#code DeelitAccessManager: https://basescan.org/address/0x0bd9338f607fbf251e5939073783c8ebdbd65bba#code DAOProxy: https://basescan.org/address/0x5cfD49Bd1d63Ec2C5d5ED554FcCf6F9e0498a3D3#code DAO:https://basescan.org/address/0x1c28432f63e034bd9522395c14ab20433397bcf6#code TokenProxy: https://basescan.org/address/0x8c6934468E41B5c041a0dE70788319BBcad6089E#code Token: https://basescan.org/address/0xdd281b901b4fc241b1b0acd1be8bc8a8842d7bb0#code LotteryProxy: https://basescan.org/address/0x336C021524766Ef43c82c7D812979e130312Fb07#code Lottery: https://basescan.org/address/0xa0401b3cae84f998924d119accc35d0e64f54cf3#code DeelitProtocolProxy: https://basescan.org/address/0x469dd47E5834fa299126403Aa89Fa9D22A46a262#code DeelitProtocol: https://basescan.org/address/0xa068436dc4970e3f7a9592c3d5be4fb0705d5b81#code RandomProducerChainlinkVRFv25:https://basescan.org/address/0x00008e12693ae4643DF25bBe97895Ee65e35DDE4#code
Commit	N/A
Unit Tests	Provided

Social Medias

Telegram	N/A
Twitter	https://x.com/Deelit_Network
Facebook	N/A
Instagram	N/A
Github	N/A
Reddit	N/A
Medium	N/A
Discord	https://discord.com/invite/rh8b9zfvTu
Youtube	N/A
TikTok	N/A
LinkedIn	N/A

Audit Summary

Version	Delivery Date	Changelog
v1.0	10. October 2024	• Layout Project • Automated- /Manual-Security Testing • Summary
v1.2	24. October 2024	• Reaudit

Note - The following audit report presents a comprehensive security analysis of the smart contract utilized in the project that includes malicious outside manipulation of the contract's functions. This analysis did not include functional testing (or unit testing) of the contract/s logic. We cannot guarantee 100% logical correctness of the contract as we did not functionally test it. This includes internal calculations in the formulae used in the contract.

File Overview

The Team provided us with the files that should be tested in the security assessment. This audit covered the following files listed below with an SHA-1 Hash.

File Name	SHA-1 Hash
DeeAO.sol	ccc94df9b1b61c9de91610b298d1251972518070
RandomProducerChainlinkVRFv25.sol	2c42d196ee1666f35982ba8a3a3aeaac1ea2cf0f
DeeToken.sol	7eb4bca656eb4a6a3dde516e2c18b17552ab7b57
DeelitAccessManager.sol	1cf44ff243bf6358d7f8f52e491e52f7b7722506
TransfertManager.sol	7eb4bca656eb4a6a3dde516e2c18b17552ab7b57
Lottery.sol	79951ecca50759b29f932e9d5c1c459ffaa58807
DeelitProtocol.sol	951b68388514d34029937c4f08d6454f77c11a82

Please note: Files with a different hash value than in this table have been modified after the security check, either intentionally or unintentionally. A different hash value may (but need not) indicate a changed state or potential vulnerability that was not the subject of this scan.

Imported packages

Used code from other Frameworks/Smart Contracts (direct imports).

Dependency / Import Path	Count
@chainlink/contracts/src/v0.8/shared/interfaces/LinkTokenInterface.sol	1
@chainlink/contracts/src/v0.8/vrf/dev/VRFConsumerBaseV2Plus.sol	1
@chainlink/contracts/src/v0.8/vrf/dev/libraries/VRFV2PlusClient.sol	1
@openzeppelin/contracts-upgradeable/access/manager/AccessManagedUpgradeable.sol	4
@openzeppelin/contracts-upgradeable/access/manager/AccessManagerUpgradeable.sol	1
@openzeppelin/contracts-upgradeable/governance/GovernorUpgradeable.sol	1
@openzeppelin/contracts-upgradeable/governance/extensions/GovernorCountingSimpleUpgradeable.sol	1
@openzeppelin/contracts-upgradeable/governance/extensions/GovernorSettingsUpgradeable.sol	1
@openzeppelin/contracts-upgradeable/governance/extensions/GovernorStorageUpgradeable.sol	1
@openzeppelin/contracts-upgradeable/governance/extensions/GovernorTimelockControlUpgradeable.sol	1
@openzeppelin/contracts-upgradeable/governance/extensions/GovernorVotesUpgradeable.sol	1
@openzeppelin/contracts-upgradeable/proxy/utils/Initializable.sol	3
@openzeppelin/contracts-upgradeable/proxy/utils/UUPSUpgradeable.sol	4
@openzeppelin/contracts-upgradeable/token/ERC20/ERC20Upgradeable.sol	1
@openzeppelin/contracts-upgradeable/token/ERC20/extensions/ERC20BurnableUpgradeable.sol	1
@openzeppelin/contracts-upgradeable/token/ERC20/extensions/ERC20PermitUpgradeable.sol	1
@openzeppelin/contracts-upgradeable/token/ERC20/extensions/ERC20VotesUpgradeable.sol	1
@openzeppelin/contracts-upgradeable/utils/ContextUpgradeable.sol	2
@openzeppelin/contracts-upgradeable/utils/NoncesUpgradeable.sol	1
@openzeppelin/contracts-upgradeable/utils/PausableUpgradeable.sol	2
@openzeppelin/contracts-upgradeable/utils/cryptography/EIP712Upgradeable.sol	2
@openzeppelin/contracts/access/manager/AccessManaged.sol	1

@openzeppelin/contracts/access/manager/IAccessManager.sol	3
@openzeppelin/contracts/governance/utils/IVotes.sol	1
@openzeppelin/contracts/token/ERC20/IERC20.sol	2
@openzeppelin/contracts/token/ERC20/utils/SafeERC20.sol	2
@openzeppelin/contracts/utils/Address.sol	2
@openzeppelin/contracts/utils/Nonces.sol	1
@openzeppelin/contracts/utils/cryptography/ECDSA.sol	1
@openzeppelin/contracts/utils/cryptography/SignatureChecker.sol	1
@openzeppelin/contracts/utils/math/Math.sol	2
@openzeppelin/contracts/utils/structs/BitMaps.sol	1

Note for Investors: We only audited contracts mentioned in the scope above. All contracts related to the project apart from that are not a part of the audit, and we cannot comment on its security and are not responsible for it in any way.

Audit Information

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. The 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 check the repository for security-related issues, code quality, and compliance with specifications and best practices. To this end, our team of experienced pen-testers and smart contract developers reviewed the code line by line and documented any issues discovered.

We check every file manually. We use automated tools only so that they help us achieve faster and better results.

Methodology

The auditing process follows a routine series of steps:

1. Code review that includes the following:
    a. Review the specifications, sources, and instructions provided to SolidProof to ensure we understand the smart contract's size, scope, and functionality.
    b. Manual review of the code, i.e., reading the source code line by line to identify potential vulnerabilities.
    c. Comparison to the specification, i.e., verifying that the code does what is described in the specifications, sources, and instructions provided to SolidProof.

2. Testing and automated analysis that includes the following:
    a. Test coverage analysis determines whether test cases cover code and how much code is executed when those test cases are executed.
    b. Symbolic execution is analysing a program to determine what inputs cause each part of a program to execute.

3. Review best practices, i.e., smart contracts to improve efficiency, effectiveness, clarity, maintainability, security, and control based on best practices, recommendations, and research from industry and academia.

4. Concrete, itemized and actionable recommendations to help you secure your smart contracts.

Overall Security

Upgradeability

Contract is an upgradeable	❌ Deployer can update the contract with new functionalities
Description	The deployer can replace the old contract with a new one with new features. Be aware of this, because the owner can add new features that may have a negative impact on your investments.
Example	We assume that you have funds in the contract and it has been audited by any security audit firm. Now the audit has passed. After that, the deployer can upgrade the contract to allow him to transfer the funds you purchased without any approval from you. This has the consequence that your funds can be taken by the creator.
Comment	The contract contains the functionality in which the deployer can update and deploy a new version of the contract s after the initial deployment.

Ownership

The ownership is not renounced	❌ The ownership is not renounced
Description	The owner has not renounced the ownership that means that the owner retains control over the contract's operations, including the ability to execute functions that may impact the contract's users or stakeholders. This can lead to several potential issues, including: • Centralizations • The owner has significant control over contract's operations
Example	We assume that you have funds in the contract and it has been audited by any security audit firm. Now the audit has passed. After that, the deployer can upgrade the contract to allow him to transfer the funds you purchased without any approval from you. This has the consequence that your funds can be taken by the creator.
Comment	N/A

Note - If the contract is not deployed then we would consider the ownership to be not renounced. Moreover, if there are no ownership functionalities then the ownership is automatically considered renounced.

Ownership Privileges

These functions can be dangerous. Please note that abuse can lead to financial loss. We have a guide where you can learn more about these Functions.

Minting tokens

Minting tokens refers to the process of creating new tokens in a cryptocurrency or blockchain network. This process is typically performed by the project's owner or designated authority, who can add new tokens to the network's total supply.

Contract owner cannot mint new tokens	✅ **The owner cannot mint new tokens**
Description	The owner is not able to mint new tokens once the contract is deployed.
Comment	N/A

Burning Tokens without Allowance

Burning tokens is the process of permanently destroying a certain number of tokens, reducing the total supply of a cryptocurrency or token. This is usually done to increase the value of the remaining tokens, as the reduced supply can create scarcity and potentially drive up demand.

Contract owner cannot burn tokens	✅ **The owner cannot burn tokens**
Description	The owner is not able burn tokens without any allowances.
Comment	N/A

Blacklist addresses

Blacklisting addresses in smart contracts is the process of adding a certain address to a blacklist, effectively preventing them from accessing or participating in certain functionalities or transactions within the contract. This can be useful in preventing fraudulent or malicious activities, such as hacking attempts or money laundering.

Contract owner cannot blacklist addresses	✅ **The owner cannot blacklist addresses**
Description	The owner is not able blacklist addresses to lock funds.
Comment	N/A

Fees and Tax

In some smart contracts, the owner or creator of the contract can set fees for certain actions or operations within the contract. These fees can be used to cover the contract's cost, such as paying for gas fees or compensating the contract's owner for their time and effort in developing and maintaining the contract.

Contract owner cannot set fees more than 25%	✅ **The owner cannot levy unfair taxes**
Description	The owner is not able to set the fees above 25%.
Comment	N/A

Lock User Funds

In a smart contract, locking refers to the process of restricting access to certain tokens or assets for a specified period of time. When tokens or assets are locked in a smart contract, they cannot be transferred or used until the lock-up period has expired or certain conditions have been met.

Contract owner can lock the user funds	❌ **The owner is able to lock the contract**
Description	Locking the contract means that the owner is able to lock any funds of addresses that they are not able to transfer bought tokens anymore.
Example	An example of locking is by pausing the contract or blacklisting any addresses. That causes that the blacklisted address is not able to transfer (buy/sell) anymore.
Comment	N/A

File/Line(s): L492-494
Codebase: Lottery.sol

```
ftrace | funcSig
function pause() external restricted {
    _pause();
}
```

File/Line(s): L261-263
Codebase: DeelitProtocol.sol

```
/// @dev Pause the protocol.
ftrace | funcSig
function pause() external restricted {
    _pause();
}
```

External/Public functions

External/public functions are functions that can be called from outside of a contract, i.e., they can be accessed by other contracts or external accounts on the blockchain. These functions are specified using the function declaration's external or public visibility modifier.

State variables

State variables are variables that are stored on the blockchain as part of the contract's state. They are declared at the contract level and can be accessed and modified by any function within the contract. State variables can be defined with a visibility modifier, such as public, private, or internal, which determines the access level of the variable.

Components

📝Contracts	📚Libraries	🔍Interfaces	🎨Abstract
6	0	0	1

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
53	3

External	Internal	Private	Pure	View
39	85	11	4	36

StateVariables

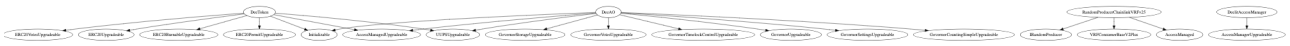
Total	🌐Public
21	14

Capabilities

Solidity Versions observed	Transfers ETH	💰 Can Receive Funds	🖥️ Uses Assembly	💣 Has Destroyable Contracts
^0.8.20 0.8.24		yes	yes (2 asm blocks)	

Inheritance Graph

An inheritance graph is a graphical representation of the inheritance hierarchy among contracts. In object-oriented programming, inheritance is a mechanism that allows one class (or contract, in the case of Solidity) to inherit properties and methods from another class. It shows the relationships between different contracts and how they are related to each other through inheritance.



Centralization Privileges

Centralization can arise when one or more parties have privileged access or control over the contract's functionality, data, or decision-making. This can occur, for example, if a single entity controls the contract or if certain participants have special permissions or abilities that others do not.

In the project, some authorities have access to the following functions:

File	Privileges
RandomPProducerChainlinkVRFv25.sol	• The restricted wallets can update the callback gas limit to any arbitrary value in the contract. • The restricted wallets can update the confirmation requests value in the contract. • The restricted wallets can enable/disable native payment method. • The restricted wallets can update the gas lane hash key.
Lottery.sol	• The restricted wallets can update the protocol contract address in the contract. • The restricted wallets can update the minimum vesting period to any arbitrary value in the contract. • The restricted wallets can update the random producer contract address. • The restricted wallets can pause and un-pause the redeem and pay functionality in the contract.
DeelitProtocol.sol	• The restricted wallets can set any fees in the contract. • The restricted wallets can pause/un-pause the functions in the contract.

Recommendations

To avoid potential hacking risks, the client should manage the private key of the privileged account with care. Additionally, we recommend enhancing the security practices of centralized privileges or roles in the protocol through a decentralized mechanism or smart-contract-based accounts, such as multi-signature wallets.

Here are some suggestions of what the client can do:

- Consider using multi-signature wallets: Multi-signature wallets require multiple parties to sign off on a transaction before it can be executed, providing an extra layer of security, e.g. Gnosis Safe
- Use of a timelock at least with a latency of, e.g. 48-72 hours for awareness of privileged operations
- Introduce a DAO/Governance/Voting module to increase transparency and user involvement
- Consider Renouncing the ownership so that the owner can no longer modify any state variables of the contract. Make sure to set up everything before renouncing.

Audit Results

Critical issues

No critical issues

High issues

No high issues

High issues

#1 | The owner can lock claim.

File	Severity	Location	Status
Lottery.sol	Medium	L492-494	ACK
DeelitProtocol.sol	Medium	L261-263	ACK

Description - The contract contains the functionality in which the restricted users in the contract can pause the functionality in the contract for an indefinite period of time which is not recommended as this can lock the claim and redeem functionality in the contract and user will not be able to claim their tokens.

#2 | The owner can set fees more than 25%.

File	Severity	Location	Status
DeelitProtocol.sol	Medium	L64-67	Fixed

Description - The restricted wallets can set any arbitrary value in the fees which is not recommended as this can lock the contract if the fees more than 25% in the contract. There must be a check so that the fees in the contract should not be more than 25%.

#3 | Missing Threshold.

File	Severity	Location	Status
Lottery.sol	Medium	L116-118	ACK

Description - The restricted wallet can set any arbitrary value in the minimum vesting period in the contract which is not recommended as if the value is set to any excessive number the functionality will be locked till that period of time. There must be a check so that the minimum value cannot be set to any arbitrary number to avoid this circumstances in the contract.

Low issues

#1 | MissingThreshold.

File	Severity	Location	Status
RandomProducerChainlinkVRFv25.sol	Low	L70-72, L74-76	Fixed

Description -The restricted wallets can update any arbitrary value in the gas limit and confirmation request including zero which is not recommended as this can cause the failure of functionality if the value is set incorrectly. There must be a check so that the parameters in the contract should be added correctly in the contract.

#2 | Missing Events

File	Severity	Location	Status
RandomProducerChainlinkVRFv25.sol	Low	L70-72, L74-76, L78-80, L82-84, L86-88	Fixed

Description - Make sure to emit events for all the critical parameter changes in the contract to ensure the transparency and trackability of all the state variable changes.

Informational issues

#1 | NatSpec documentation missing

File	Severity	Location	Status
All	Informational	—	Fixed

Description - If you started to comment on your code, comment on all other functions, variables etc.

Legend for the Issue Status

Attribute or Symbol	Meaning
Open	The issue is not fixed by the project team.
Fixed	The issue is fixed by the project team.
Acknowledged(ACK)	The issue has been acknowledged or declared as part of business logic.

Blockchain Security | Smart Contract Audits | KYC Development | Marketing

MADE IN GERMANY