CERTIK

Sienna

Wrapped

Security Assessment

March 19th, 2021

Audited By:
Georgios Delkos @ CertiK
georgios.delkos@certik.io
Reviewed By:
Alex Papageorgiou @ CertiK
alex.papageorgiou@certik.org

Disclaimer

CertiK 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 or project that contracts CertiK to perform a security review.

CertiK Reports 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 technologies proprietors, business, business model or legal compliance.

CertiK Reports 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.

CertiK 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. 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.

What is a CertiK report?

- A document describing in detail an in depth analysis of a particular piece(s) of source code provided to CertiK by a Client.
- An organized collection of testing results, analysis and inferences made about the structure, implementation and overall best practices of a particular piece of source code.
- Representation that a Client of CertiK has completed a round of auditing with the intention to increase the quality of the company/product's IT infrastructure and or source code.

Overview

Project Summary

Project Name	Sienna - Wrapped
Description	A wrapped token.
Platform	Ethereum; Solidity, Yul
Codebase	N/A
Commits	1. 0dd716208636d11f86e067cb3f700ff4e7cfcd54

Audit Summary

Delivery Date	March 19th, 2021
Method of Audit	Static Analysis, Manual Review
Consultants Engaged	2
Timeline	March 8th, 2021 - March 19th, 2021

Vulnerability Summary

Total Issues	3
Total Critical	0
Total Major	0
Total Medium	0
Total Minor	1
Total Informational	2

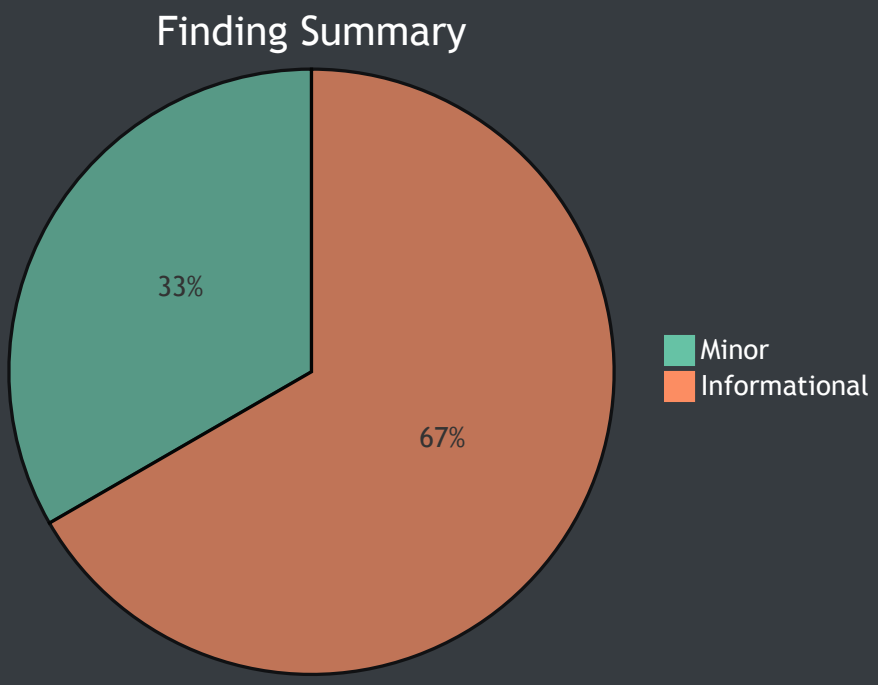
Executive Summary

Sienna requested for CertiK to perform an audit in their new smart contract system implementation. The auditing team conducted the audit in the timeframe between March 8th, 2021, and March 9th, 2021, with two engineers. The auditing process evaluated code implementation against provided specifications, examining language-specific issues, and performed manual examination of the code. The code's examination revealed issues that the auditing team discussed with the development team and were all addressed in the alleviation iteration.

Files In Scope

ID	Contract	Location
WSA	WrappedSienna.sol	contracts/WrappedSienna.sol

File Dependency Graph



Manual Review Findings

ID	Title	Type	Severity	Resolved
WSA-01	Potentially Unwanted Side-Effect	Language Specific	Minor	✓
WSA-02	Unlocked Compiler Version	Language Specific	Informational	✓
WSA-03	Redundant Virtual Marker	Language Specific	Informational	✓

WSA-01: Potentially Unwanted Side-Effect

Type	Severity	Location
Language Specific	Minor	WrappedSienna.sol L77

Description:

A potentially unwanted side effect of the _transfer function being overriden is that a transferFrom a minter to any user would cause tokens to be minted as _transfer is also being utilized during the execution of transferFrom in the ERC20 standard of OpenZeppelin.

Recommendation:

We advise that this behavior is evaluated and if identified to be undesirable, the transferFrom function is overridden to account for this fact.

Alleviation:

The team has addresed the issue in rc2.

WSA-02: Unlocked Compiler Version

Type	Severity	Location
Language Specific	Informational	WrappedSienna.sol L3

Description:

The contract has unlocked compiler version. An unlocked compiler version in the source code of the contract permits the user to compile it at or above a particular version. This, in turn, leads to differences in the generated bytecode between compilations due to differing compiler version numbers. This can lead to an ambiguity when debugging as compiler specific bugs may occur in the codebase that would be hard to identify over a span of multiple compiler versions rather than a specific one.

Recommendation:

We advise that the compiler version is instead locked at the lowest version possible that the contract can be compiled at. For example, for version `v0.6.2` the contract should contain the following line:

```
pragma solidity 0.6.2;
```

Alleviation:

The team has addresed the issue in rc2.

WSA-03: Redundant Virtual Marker

Type	Severity	Location
Language Specific	Informational	WrappedSienna.sol L63, L77

Description:

The code contains the virtual marker for both functions while that is not required.

Recommendation:

We advise to remove the virtual marker.

Alleviation:

The team has addresed the issue in rc2.

Appendix

Finding Categories

Language Specific

Language Specific findings are issues that would only arise within Solidity, i.e. incorrect usage of `private` or `delete`.