Security Assessment

Sienna Rewards Release

Aug 23rd, 2021

Table of Contents

Summary

Overview

- Project Summary
- Audit Summary
- Vulnerability Summary
- Audit Scope

Findings

- SNK-01 : Misleading Error Message
- SNR-01 : Fields Out Of Order
- SNR-02 : Redundant Use Of Some
- SNR-03 : Misleading Error Message
- SNT-01 : Rounding Issue

Appendix

Disclaimer

About

Summary

This report has been prepared for Sienna to discover issues and vulnerabilities in the source code of the Sienna Rewards Release project as well as any contract dependencies that were not part of an officially recognized library. A comprehensive examination has been performed, utilizing Static Analysis and Manual Review techniques.

The code in scope for the most part is well orchestrated with good language usage and respect to language-specific best practices.

All issues identified were addressed by the team in release 2.1.1.

Overview

Project Summary

Project Name	Sienna Rewards Release
Description	Rewards
Platform	CosmosSDK
Language	Rust
Codebase	https://github.com/SiennaNetwork/sienna
Commit	314da73b59eec7b5cca1cb12c1b7a009fb1dd196

Audit Summary

Delivery Date	Aug 23, 2021
Audit Methodology	Static Analysis, Manual Review
Key Components	

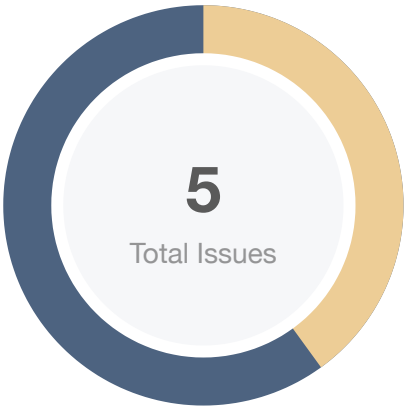
Vulnerability Summary

Vulnerability Level	Total	Pending	Declined	Acknowledged	Partially Resolved	Resolved
Critical	0	0	0	0	0	0
Major	0	0	0	0	0	0
Medium	0	0	0	0	0	0
Minor	2	0	0	0	0	2
Informational	3	0	0	0	0	3
Discussion	0	0	0	0	0	0

Audit Scope

ID	Repo	Commit	File	SHA256 Checksum
CSN	SiennaNetwork/sienna	314da73	rewards/Cargo.toml	a0823c6fb14a03581d960576524171d7fca3d0ea97e33142d265c93439140119
SNK	SiennaNetwork/sienna	314da73	rewards/rewards.rs	136512fdd2f3ecf693aa297bf7347d03e446e141fb7f7691ff2b67c18bebe2ca
SNR	SiennaNetwork/sienna	314da73	rewards/rewards_algo.rs	8bd87ed2388ece7c26d3a201b30428c916aef9e4289c6a5d66c5e5575f05b629
SNO	SiennaNetwork/sienna	314da73	rewards/rewards_config.rs	0869085e75db7f823093d300c961f254754038d7e98446070c410c49783246dd
SNW	SiennaNetwork/sienna	314da73	rewards/rewards_harness.rs	3152e8d5a07f1234f3b88351f9ece7f01abf948bbd0c5ec9a49a1f3132e6fea0
SNT	SiennaNetwork/sienna	314da73	rewards/rewards_math.rs	275b460fb84f811d8b02d46d03316b3da9a95cfac400fd39ba837f3508e67ac7
SNE	SiennaNetwork/sienna	314da73	rewards/rewards_test.rs	5a58c90731e83932dc4c591cd6bbfb8af105fb3496632efc470ed7dbef38ffb9

Findings



Critical	0 (0.00%)
Major	0 (0.00%)
Medium	0 (0.00%)
Minor	2 (40.00%)
Informational	3 (60.00%)
Discussion	0 (0.00%)

ID	Title	Category	Severity	Status
SNK-01	Misleading Error Message	Logical Issue	Minor	Resolved
SNR-01	Fields Out Of Order	Coding Style	Informational	Resolved
SNR-02	Redundant Use Of Some	Language Specific, Coding Style	Informational	Resolved
SNR-03	Misleading Error Message	Logical Issue	Minor	Resolved
SNT-01	Rounding Issue	Logical Issue, Mathematical Operations	Informational	Resolved

SNK-01 | Misleading Error Message

Category	Severity	Location	Status
Logical Issue	Minor	rewards/rewards.rs: 158, 173	Resolved

Description

The linked error message is misleading and does not provide enough information about the issue.

Recommendation

Consider refactoring the error message to something more explanatory.

Alleviation

The issue was addressed by the team in release 2.1.1.

SNR-01 | Fields Out Of Order

Category	Severity	Location	Status
Coding Style	Informational	rewards/rewards_algo.rs: 112	Resolved

Description

The function return struct contains all the fields but not in a proper order degrading the readability of the code base.

Recommendation

Consider refactoring the code and keep the order of the fields.

Alleviation

The issue was addressed by the team in release 2.1.1.

SNR-02 | Redundant Use Of Some

Category	Severity	Location	Status
Language Specific, Coding Style	Informational	rewards/rewards_algo.rs: 134, 303	Resolved

Description

The linked function creates redundant allocation to check if an option contains a value.

Recommendation

Consider using `is_some()`.

Alleviation

The issue was addressed by the team in release 2.1.1.

SNR-03 | Misleading Error Message

Category	Severity	Location	Status
Logical Issue	Minor	rewards/rewards_algo.rs: 310, 480	Resolved

Description

The linked error message is misleading and does not provide enough information about the issue.

Recommendation

Consider refactoring the error message to something more explanatory.

Alleviation

The issue was addressed by the team in release 2.1.1.

SNT-01 | Rounding Issue

Category	Severity	Location	Status
Logical Issue, Mathematical Operations	Informational	rewards/rewards_math.rs: 36	Resolved

Description

The linked code contains a call to the `multiply_ratio` function that could lead to rounding issues based on the comments that are present to the underlying function.

Recommendation

Consider creating dedicated test to ensure the intended outcome.

Alleviation

The issue was addressed by the team in release 2.1.1.

Appendix

Finding Categories

Mathematical Operations

Mathematical Operation findings relate to mishandling of math formulas, such as overflows, incorrect operations etc.

Logical Issue

Logical Issue findings detail a fault in the logic of the linked code, such as an incorrect notion on how block.timestamp works.

Language Specific

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

Coding Style

Coding Style findings usually do not affect the generated byte-code but rather comment on how to make the codebase more legible and, as a result, easily maintainable.

Checksum Calculation Method

The "Checksum" field in the "Audit Scope" section is calculated as the SHA-256 (Secure Hash Algorithm 2 with digest size of 256 bits) digest of the content of each file hosted in the listed source repository under the specified commit.

The result is hexadecimal encoded and is the same as the output of the Linux "sha256sum" command against the target file.

Disclaimer

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 CertiK's 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 CertiK 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. 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.

The assessment services provided by CertiK 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, CERTIK HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS. WITHOUT LIMITING THE FOREGOING, CERTIK 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, CERTIK 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 ANY OTHER 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 FOREGOING, CERTIK PROVIDES NO WARRANTY OR UNDERTAKING, AND MAKES NO REPRESENTATION OF ANY KIND THAT THE SERVICE 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 CERTIK NOR ANY OF CERTIK'S AGENTS MAKES ANY REPRESENTATION OR WARRANTY OF ANY KIND, EXPRESS OR IMPLIED AS TO THE ACCURACY, RELIABILITY, OR CURRENCY OF ANY INFORMATION OR CONTENT PROVIDED THROUGH THE SERVICE. CERTIK 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 OWNER OR DISTRIBUTOR OF THE THIRD-PARTY MATERIALS.

THE SERVICES, ASSESSMENT REPORT, AND ANY OTHER MATERIALS HEREUNDER 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 CERTIK'S 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 CERTIK WITH RESPECT TO SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING MATERIALS.

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

About

Founded in 2017 by leading academics in the field of Computer Science from both Yale and Columbia University, CertiK is a leading blockchain security company that serves to verify the security and correctness of smart contracts and blockchain-based protocols. Through the utilization of our world-class technical expertise, alongside our proprietary, innovative tech, we're able to support the success of our clients with best-in-class security, all whilst realizing our overarching vision; provable trust for all throughout all facets of blockchain.