Security Assessment

Soda Protocol

Oct 26th, 2021

Table of Contents

Summary

This report has been prepared for Soda Protocol to locate potential vulnerabilities and thereafter verify the correctness of specific components in said project's source code. A series of thorough security assessments have been performed utilizing the Manual Review and Fuzzing technique(s), the goal of which is to help the client protect their users through discovering, mitigating and ultimately fixing security flaws that could lead to unauthorized access, loss of funds, cascading failures, and/or other vulnerabilities. Alongside each security finding a recommendation on fixes and/or mitigation methods are also given.

Overview

Project Summary

Project Name	Soda Protocol
Platform	Solana
Language	Rust
Codebase	https://github.com/soda-protocol/soda-contract-lending
Commit	1c12d55ade82906dfe3f6a3af4517918f7d29a4f

Audit Summary

Delivery Date	Oct 26, 2021
Audit Methodology	Manual Review, Fuzzing
Key Components	Lending

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	2	0	0	1	0	1
Minor	4	0	0	1	0	3
Informational	1	0	0	1	0	0
Discussion	0	0	0	0	0	0

Audit Scope

ID	File	SHA256 Checksum
COM	projects/soda-lending-contract-audit/program/src/math/common.rs	d0bd8c0f8ddbc1f4162756d8e411b1a9f4325f13cc2c0dca94bca3ec49190493
DEC	projects/soda-lending-contract-audit/program/src/math/decimal.rs	1300ced1f4788c6f57704b46a8b43e1d8c00900a0959ad41c8982b26d74d8a91
MOD	projects/soda-lending-contract-audit/program/src/math/mod.rs	3832216d2453d6ca4bd9526910ed92663850e40f017a1a79c5e1ae50ae980245
RAT	projects/soda-lending-contract-audit/program/src/math/rate.rs	c4cc5adddf10470a0a0f3a7e77550189c2460cbf1fb52f1859c059fc2df7f8de
CHA	projects/soda-lending-contract-audit/program/src/oracle/chainlink.rs	de31bd4c55fab31d19dcf7bf5abd0c6ddd7dcbc65949ec0117ff9d155149c3c4
MOO	projects/soda-lending-contract-audit/program/src/oracle/mod.rs	4887c249c7e0fb305713fd2708398aec4d9683f494c612ae6a83ed7683b71b62
PYT	projects/soda-lending-contract-audit/program/src/oracle/pyth.rs	6fc2cea0c769c8234aab5871aabac577b5acc51cf746f834d3ca71597ab7b3b4
SWI	projects/soda-lending-contract-audit/program/src/oracle/switchboard.rs	5acc825d6a2f8d6180e6f2994875972bfe4863767cb25f5acf7d6e0c0305bccd
LAS	projects/soda-lending-contract-audit/program/src/state/last_update.rs	1cf9dcfdb97d02720f3281dc361d88684baa18a6aec85d3c6d95917464978a0d
MAN	projects/soda-lending-contract-audit/program/src/state/manager.rs	5a73b3d22bad2da9ec5a8486e1df1fc48d7a3fbd3de8102a2377634d30f6f12e
MAR	projects/soda-lending-contract-audit/program/src/state/market_reserve.rs	2d1f7e020280fdbe689eb4f27f6afdc57d097a9e00aa63010ec870a3962823b6
MOS	projects/soda-lending-contract-audit/program/src/state/mod.rs	737cbd8051131097632707390178949660 9c93e6f35d92e87a6cf76482cd8bb1
RAE	projects/soda-lending-contract-audit/program/src/state/rate_model.rs	60551892d08c7d5ce3ae1c79e9272928515408dcb69f9cb0a0c59fa729b13a49
UNI	projects/soda-lending-contract-audit/program/src/state/unique_credit.rs	d4f88243b0db26b4d1bc66989cdbb0a09f508c6e199a638942ce9a0636eb795b

ID	File	SHA256 Checksum
USE	projects/soda-lending-contract-audit/program/src/state/user_obligation.rs	845cc2d7a2cd0644d374b203c2427cbd64821eb9c6f16e6411e41bda2c79a6f3
ENT	projects/soda-lending-contract-audit/program/src/entrypoint.rs	f933338463dedd95d7d97d9a82bea938baf156d3cc980117fe2db53cd4878850
ERR	projects/soda-lending-contract-audit/program/src/error.rs	e33f5912cdd73e9df7336e9729630dac5d95d5c9a1676ef0c2ea9e4eb040775b
INS	projects/soda-lending-contract-audit/program/src/instruction.rs	aa4f0535bb5c147a260fb61052736996749fdf632cda95eea721642aa02f3f3a
LIB	projects/soda-lending-contract-audit/program/src/lib.rs	9abc20ecda897391577e53ead214c43e5d629532a39c64643e2e5bce15ec806b
PRO	projects/soda-lending-contract-audit/program/src/processor.rs	fe10b93c8e660b3a0b07ab0c2136da0339f9950da23b6a31310eb41769b2acef
CCK	projects/soda-lending-contract-audit/program/Cargo.toml	ab7e340d8a8e6209b434d64b7977e75ddcf41930f06d4f38aeaf93745822ecd5

Review Notes

Our audit approach primarily revolves around a multi-round manual review process, and largely favors modularity and encapsulation in code design. At a high level we analyze each object (or module) by their interfaces and references to other objects. This ultimately ensures that the same security properties can be extended to new objects added to the system, which in return minimizes the attack surface of the application down to the implementation of specific objects.

Additionally we analyze how the state machines are defined and how state transitions are triggered, the focus of which is to check the implementation against the specs (if provided) and hence mitigate the possibilities of unintentional state behaviors taking place.

Key Checks

Common Vulnerabilities

- Constants precision and conversion
- Integer overflow/underflow
- Stack overflow
- Index Out-of-Bound
- Out-of-Memory

Ownership

- Moves (e.g. control flow, indexed content)
- Shared ownership (e.g. reference-counted pointer types)

References

- Sharing and mutation
- Borrowing references
- Receiving references as parameters
- Returning references

Composition

- Type grouping
- Cascading changes

Decoupling

- Semantic consistency
- Indirection and allocation cost
- Type coercion
- Trait pollution

Error Handling

- Unwrapping, logging and propagating errors
- Panics (e.g. detection, unwinding and recovery)

Unsafe Code

- Undefined behaviors (e.g. memory leaks, use after fee, double free)
- Exception safety
- Uninitialized memory
- Data races

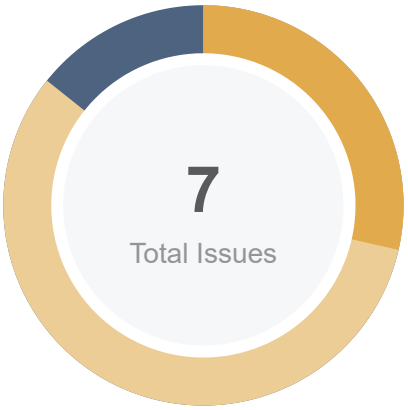
Advanced Vulnerabilities

- Format string attacks
- Cryptographic attacks (e.g. timing attacks)

General Checks

- Organization of crates and modules
- Language best practices

Findings



Critical	**0** (0.00%)
Major	**0** (0.00%)
Medium	**2** (28.57%)
Minor	**4** (57.14%)
Informational	**1** (14.29%)
Discussion	**0** (0.00%)

ID	Title	Category	Severity	Status
MOS-01	Max Parameter Used Inconsistently	Mathematical Operations, Magic Numbers	Medium	Acknowledged
PRO-01	Approve Instead of Transfer for Liquidation	Logical Issue	Medium	Resolved
PRO-02	Accruing Interest Right After Borrow	Logical Issue	Minor	Resolved
PRO-03	No Amount Validation for Borrow Liquidity By Unique Credit	Control Flow	Minor	Resolved
PRO-04	No Amount Validation for Reduce Insurance	Logical Issue	Minor	Resolved
USE-01	Division Before Multiplication	Mathematical Operations	Minor	Acknowledged
USE-02	Redundant Statement	Logical Issue, Data Flow	Informational	Acknowledged

MOS-01 | Max Parameter Used Inconsistently

Category	Severity	Location	Status
Mathematical Operations, Magic Numbers	Medium	projects/soda-lending-contract-audit/program/src/state/mod.rs: 160~162, 169~170	Acknowledged

Description

Function `calculate_amount` and `calculate_amount_and_decimal` accept two inputs, `amount` and `max` respectively, and returns `max` if and only if `amount == u64::MAX`. This is not intuitive or necessary.

Recommendation

Refrain from using `u64::MAX` as a flag to return the max possible value. Instead consider using the `Option<u64>` type for `amount` and returning `max` if the input is `None`.

Alleviation

The Soda Protocol team responded with the following statement:

"Since input amount is directly passed by instructions, and u64::MAX means user want this amount should be as large as possibe, there is no need to change it as an option."

We agree that using u64::MAX amount as a flag to return the largest possible value is a sound option given the context and consider the exhibit fully attended to.

PRO-01 | Approve Instead of Transfer for Liquidation

Category	Severity	Location	Status
Logical Issue	Medium	projects/soda-lending-contract-audit/program/src/processor.rs: 1867~1875	Resolved

Description

Comment says to transfer but uses SPL approve *without SPL revoke*.

Recommendation

Either change to a SPL transfer or add an SPL revoke similar to `process_flash_loan` and fix the comment.

Alleviation

The recommendation was applied in commit `c8ae157`.

PRO-02 | Accruing Interest Right After Borrow

Category	Severity	Location	Status
Logical Issue	Minor	projects/soda-lending-contract-audit/program/src/processor.rs: 1849~1851	Resolved

Description

The loan market's interest is calculated right after the flash loan, which might burden the flash loan caller.

Recommendation

Accrue interest on the loan market before the flash loan processing.

Alleviation

The recommendation was applied in commit `c8ae157`.

PRO-03 | No Amount Validation for Borrow Liquidity By Unique Credit

Category	Severity	Location	Status
Control Flow	Minor	projects/soda-lending-contract-audit/program/src/processor.rs: 2134	Resolved

Description

There is no check to validate the input amount.

Recommendation

Like many other functions, return an error with an appropriate error message if `amount == 0`

Alleviation

The recommendation was applied in commit `c8ae157`.

PRO-04 | No Amount Validation for Reduce Insurance

Category	Severity	Location	Status
Logical Issue	Minor	projects/soda-lending-contract-audit/program/src/processor.rs: 2398	Resolved

Description

There is no check to validate the input amount.

Recommendation

Like many other functions, return an error with an appropriate error message if `amount == 0`

Alleviation

The recommendation was applied in commit `c8ae157`.

USE-01 | Division Before Multiplication

Category	Severity	Location	Status
Mathematical Operations	Minor	projects/soda-lending-contract-audit/program/src/state/user_obligation.rs: 647~654, 609~615, 564~571, 506~509	Acknowledged

Description

In the highlighted code divisions can be seen performed before multiplications. While this is not arithmetically incorrect, division before multiplication can sometimes cause loss of precision.

Recommendation

Perform Multiplication before division if possible to mitigate the loss of precision.

Alleviation

The Soda Protocol team responded with the following statement:

"Since we used 192bit integer as base number type, it might lead to overflow if multiplications are always done before division."

Despite potential loss of precision we agree with the team's sentiment and consider the exhibit fully attended to.

USE-02 | Redundant Statement

Category	Severity	Location	Status
Logical Issue, Data Flow	Informational	projects/soda-lending-contract-audit/program/src/state/user_obligation.rs: 344	Acknowledged

Description

Since the function `find_and_remove` will update the vector in place, it is not necessary to recreate the vector.

Recommendation

Remove the statement that reconstructs the vector.

Alleviation

The Soda Protocol team responded with the following statement:

"In Soda we allow both the same collateral and loan exist in obligations. So the reserves vector updated after seeking collaterals should not be used for seeking loans"

We agree with the team's sentiment and consider the exhibit fully attended to.

Appendix

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.