sec3™

Security Assessment Report

Monaco Protocol Product Program v0.1.0

March 27, 2023

Summary

The sec3 team (formerly Soteria) was engaged to do a thorough security analysis of the Monaco Protocol Solana smart contract at https://github.com/MonacoProtocol/protocol-product. The initial audit was done on the source code of the following version

- **Contract "protocol_product":**
  - commit 751f7c615e63f2286fe2af0a6e3b36a1231819bf

The audit revealed 1 issue. The team responded with the following commits for the post-audit review, which is to validate if the reported issues have been addressed.

  - v0.1.0, commit 5ae3e3bd7b12896a0483ef4018d6faaab6823527

This report describes the findings and resolutions in detail.

Table of Contents

Methodology and Scope of Work

The sec3 (formerly Soteria) audit team, which consists of Computer Science professors and industrial researchers with extensive experience in Solana smart contract security, program analysis, testing and formal verification, performed a comprehensive manual code review, software static analysis and penetration testing.

Assisted by the sec3 Scanner developed in-house, the audit team particularly focused on the following work items:

- Check common security issues.
    - Missing ownership checks
    - Missing signer checks
    - Signed invocation of unverified programs
    - Solana account confusions
    - Arithmetic over- or underflows
    - Numerical precision errors
    - Loss of precision in calculation
    - Insufficient SPL-Token account verification
    - Missing rent exemption assertion
    - Casting truncation
    - Did not follow security best practices
    - Outdated dependencies
    - Redundant code
    - Unsafe Rust code
- Check program logic implementation against available design specifications.
- Check poor coding practices and unsafe behavior.
- The soundness of the economics design and algorithm is out of scope of this work

Result Overview

In total, the audit team found the following issues.

MONACO PROTOCOL PRODUCT PROGRAM v0.1.0

Issue	Impact	Status
[I-1] The product title string validation can be improved	Informational	Resolved

Findings in Detail

IMPACT – INFO

[I -1] The product title string validation can be improved

The length of the PDA seed (product_title.as_ref()) should be smaller than or equal to 32. Please see solana-labs/solana/blob/272e667/sdk/program/src/pubkey.rs#L585 for more details.

It's not exploitable as the program will panic if the product_title is too long.

```
/* protocol-product/programs/protocol_product/src/state/product.rs */
impl Product {
    pub const PRODUCT_TITLE_MAX_LENGTH: usize = 50;

/* protocol-product/programs/protocol_product/src/instructions/product.rs */
pub fn create_product(
    product_title: String,
) -> Result<()> {
    validate_commission_rate(commission_rate)?;

    require!(
        (1..=50).contains(&product_title.len()), //  should be smaller than 32
        ProductError::ProductTitleLen
    );
```

Resolution

The check now makes sure empty strings will not be accepted. This issue has been resolved.

DISCLAIMER

The instance report ("Report") was prepared pursuant to an agreement between Coderrect Inc. d/b/a sec3 (the "Company") and BetDEX Labs (the "Client"). This Report solely includes the results of a technical assessment of a specific build and/or version of the Client's code specified in the Report ("Assessed Code") by the Company. The sole purpose of the Report is to provide the Client with the results of the technical assessment of the Assessed Code. The Report does not apply to any other version and/or build of the Assessed Code. Regardless of the contents of the Report, the Report does not (and should not be interpreted to) provide any warranty, representation or covenant that the Assessed Code: (i) is error and/or bug free, (ii) has no security vulnerabilities, and/or (iii) does not infringe any third-party rights. Moreover, the Report is not, and should not be considered, an endorsement by the Company of the Assessed Code and/or of the Client. Finally, the Report should not be considered investment advice or a recommendation to invest in the Assessed Code and/or the Client.

This Report is considered null and void if the Report (or any portion thereof) is altered in any manner.

ABOUT

Founded by leading academics in the field of software security and senior industrial veterans, sec3 (formerly Soteria) is a leading blockchain security company that currently focuses on Solana programs. We are also building sophisticated security tools that incorporate static analysis, penetration testing, and formal verification.

At sec3, we identify and eliminate security vulnerabilities through the most rigorous process and aided by the most advanced analysis tools.

For more information, check out our website and follow us on twitter.

sec3™