Synthetix Mirfak Release Smart Contract Audit

1. Introduction

iosiro was commissioned by Synthetix to conduct a smart contract audit of their Mirfak Release, which included audits on the following components:

- SIP-142 on 13 August, consuming 1 resource day.
- SIP-145 on 17 June, consuming 1 resource day.
- SIP-174 on 26 August and 1 September, consuming 2 resource days.

This report is organized into the following sections.

- **Section 2 - Executive Summary:** A high-level description of the findings of the audit.
- **Section 3 - Audit Details:** A description of the scope and methodology of the audit.

- **Section 4 - Design Specification:** An outline of the intended functionality of the smart contracts.
- **Section 5 - Detailed Findings:** Detailed descriptions of the findings of the audit.

The information in this report should be used to understand the risk exposure of the smart contracts, and as a guide to improving the security posture of the smart contracts by remediating the issues that were identified. The results of this audit are only a reflection of the source code reviewed at the time of the audit and of the source code that was determined to be in-scope.

The purpose of this audit was to achieve the following:

- Ensure that the smart contracts functioned as intended.
- Identify potential security flaws.

Assessing the market effect, economics, game theory, or underlying business model of the platform were strictly beyond the scope of this audit.

Due to the unregulated nature and ease of transfer of cryptocurrencies, operations that store or interact with these assets are considered very high risk with regards to cyber attacks. As such, the highest level of security should be observed when interacting with these assets. This requires a forward-thinking approach, which takes into account the new and experimental nature of blockchain technologies. There are a number of techniques that can help to achieve this, some of which are described below.

- Security should be integrated into the development lifecycle.
- Defensive programming should be employed to account for unforeseen circumstances.
- Current best practices should be followed when possible.

2. Executive Summary

This report presents the findings of smart contract audits performed by iosiro of Synthetix's Mirfak release.

SIP-142 deprecated the EtherCollateral loan functionality, as it has been replaced by multi-collateral loans. Several informal issues were raised and addressed during the audit.

SIP-145 implemented a bug fix to emit the correct amount of SNX backed debt when taking a full debt snapshot. The code change was minimal and was found to address the issue. No further issues were identified.

SIP-174 introduced a new method for removing synths from the system, without having to purge the synth supply. One informational issue was raised and acknowledged during the audit.

3. Audit Details

3.1 Scope

The source code considered in-scope for the assessment is described below. Code from all other files is considered to be out-of-scope. Out-of-scope code that interacts with in-scope code is assumed to function as intended and introduce no functional or security vulnerabilities for the purposes of this audit.

3.1.1 Synthetix SIP-142 Smart Contracts

Project Name: Synthetix
Commits: 70ef93e, 080fb4b
Files: contracts/BaseDebtCache.sol, contracts/BaseSynthetix.sol, contracts/EtherCollateral.sol, contracts/EtherCollateralsUSD.sol, contracts/EmptyEtherCollateral.sol, contracts/FeePool.sol, contracts/Issuer.sol, contracts/MultiCollateralSynth.sol

3.1.2 Synthetix SIP-145 Smart Contracts

Project Name: Synthetix
Commits: feffbc2
Files: contracts/DebtCache.sol

3.1.2 Synthetix SIP-174 Smart Contracts

Project Name: Synthetix

Commits: 3a2a3e8, 08874ec

Files: contracts/Exchanger.sol, contracts/Issuer.sol, contracts/SynthRedeemer.sol

3.2 Methodology

A variety of techniques were used in order to perform the audit. These techniques are briefly described below.

3.2.1 Code Review

The source code was manually inspected to identify potential security flaws. Code review is a useful approach for detecting security flaws, discrepancies between the specification and implementation, design improvements, and high risk areas of the system.

3.2.2 Dynamic Analysis

The contracts were compiled, deployed, and tested in a test environment, both manually and through the test suite provided. Manual analysis was used to confirm that the code operated at a functional level, and to verify the exploitability of any potential security issues identified.

3.2.3 Automated Analysis

Tools were used to automatically detect the presence of several types of security vulnerabilities, including reentrancy, timestamp dependency bugs, and transaction-ordering dependency bugs. The static analysis results were manually analyzed to remove false-positive results. True positive results would be indicated in this report. Static analysis tools commonly used include Slither, Securify, and MythX. Tools such as the Remix IDE, compilation output, and linters are also used to identify potential issues.

3.3 Risk Ratings

Each issue identified during the audit has been assigned a risk rating. The rating is determined based on the criteria outlined below.

- **High Risk** - The issue could result in a loss of funds for the contract owner or system users.

- **Medium Risk** - The issue resulted in the code specification being implemented incorrectly.
- **Low Risk** - A best practice or design issue that could affect the security of the contract.
- **Informational** - A lapse in best practice or a suboptimal design pattern that has a minimal risk of affecting the security of the contract.
- **Closed** - The issue was identified during the audit and has since been addressed to a satisfactory level to remove the risk that it posed.

4. Design Specification

The following section outlines the intended functionality of the system at a high level.

4.1 SIP-142

The specification of SIP-142 was based on commit hash f99f46f.

4.1 SIP-145

The specification of SIP-145 was based on commit hash f99f46f.

4.2 SIP-174

The specification of SIP-174 was based on commit hash f99f46f.

5. Detailed Findings

The following section includes in-depth descriptions of the findings of the audit.

5.1 High Risk

No high risk issues were present at the conclusion of the audit.

5.2 Medium Risk

No medium risk issues were present at the conclusion of the audit.

5.3 Low Risk

No low risk issues were present at the conclusion of the audit.

5.4 Informational

No informational issues were present at the conclusion of the audit.

5.5 Closed

5.5.1 Outstanding loans

SIP-142

At the time of deprecation, the `totalIssuedSynths` of the mainnet `EtherCollateralsUSD` contract was valued at 1821.26 sUSD due to underwater loans. As a result, removing the contract will increase the overall system debt by an equal amount as it will no longer be excluded from the total debt calculation.

Update

The Synthetix team acknowledged the issue.

5.5.3 Design comments (Informational)

Code simplifications

SIP-142

- BaseDebtCache.sol#L185 can be simplified to `isInvalid = anyTotalLongRateIsInvalid || anyTotalShortRateIsInvalid;`.
- BaseDebtCache.sol#L186 can be simplified to `excludedDebt = longValue.add(shortValue);`.

Update

Fixed in 080fb4b.

Improve comments

SIP-142

- BaseDebtCache.sol#L182,188 need to be renumbered.
- BaseSynthetix.sol#L90 can be removed.

Update

Fixed in 080fb4b.

Remove unnecessary code

SIP-142

The EmptyEtherCollateral.sol file can be removed as it is no longer in use.

Update

Fixed in 080fb4b.

SynthRedeemer validation

SIP-174

SynthRedeemer.sol#L79 only checks whether the sUSD balance of the redeemer contract exceeds the value of the total synth value being deprecated, but does not take into account the value of existing deprecated synths. However, this check is not strictly necessary as the issuer contract issues the requisite sUSD before deprecating the synth, so there should be no case where the redeemer does not have sufficient sUSD to be redeemed for the newly deprecated synth.

Update

The Synthetix team acknowledged the issue.