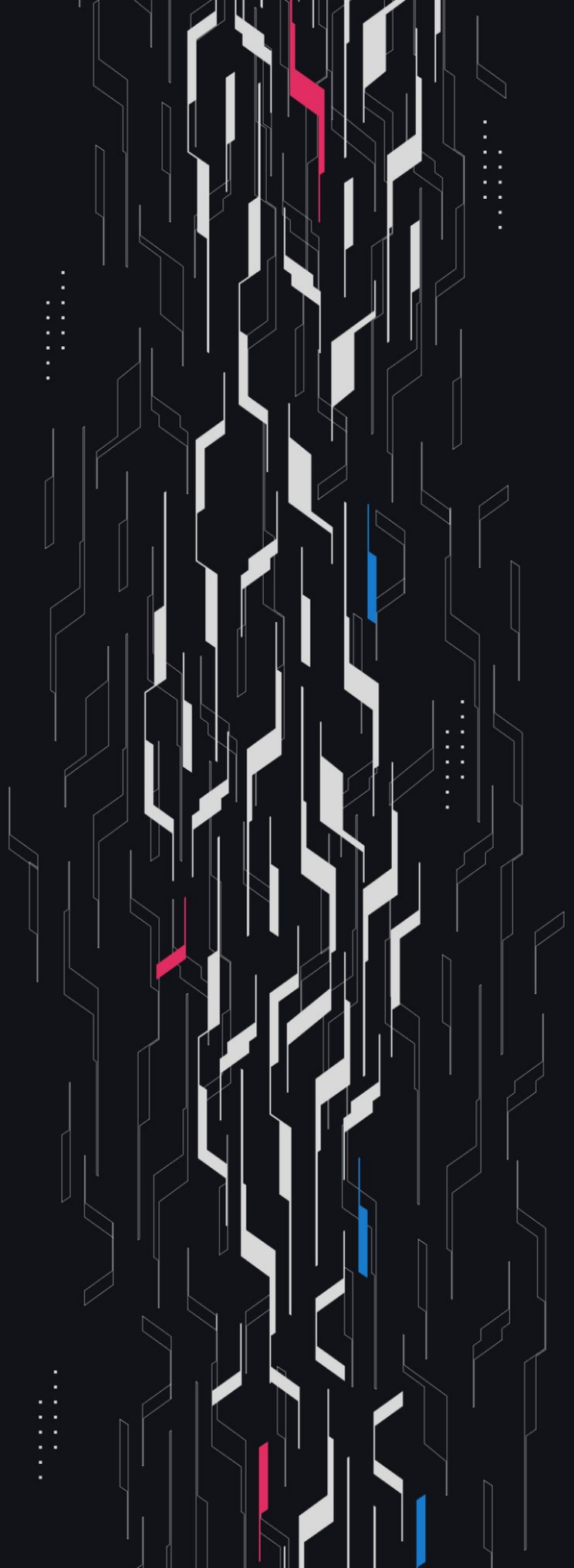
GA GUARDIAN

Synthetix

TLX Conversion

Security Assessment

December 29th, 2024



Summary

Audit Firm Guardian

Prepared By Owen Thurm, Daniel Gelfand

Client Firm Synthetix

Final Report Date December 29, 2024

Audit Summary

Synthetix engaged Guardian to review the security of its review of their TLX to SNX token conversion contract. From the 19th of December to the 23rd of December, a team of 2 auditors reviewed the source code in scope. All findings have been recorded in the following report.

For a detailed understanding of risk severity, source code vulnerability, and potential attack vectors, refer to the complete audit report below.

🔗 Blockchain network: **Optimism**

✅ Verify the authenticity of this report on Guardian's GitHub: https://github.com/guardianaudits

Table of Contents

Project Overview

Project Summary

Project Name	Synthetix
Language	Solidity
Codebase	https://github.com/bytecode-collective/synthetix-acquisition-contracts
Commit(s)	14fb7490ca92d443a0c5240a99fdd922bc2ad327

Audit Summary

Delivery Date	December 29, 2024
Audit Methodology	Static Analysis, Manual Review, Test Suite, Contract Fuzzing

Vulnerability Summary

Vulnerability Level	Total	Pending	Declined	Acknowledged	Partially Resolved	Resolved
Critical	0	0	0	0	0	0
High	0	0	0	0	0	0
Medium	0	0	0	0	0	0
Low	5	0	0	2	0	3

Audit Scope & Methodology

Vulnerability Classifications

Severity	Impact: *High*	Impact: *Medium*	Impact: *Low*
Likelihood: *High*	🔴 Critical	🟠 High	🟡 Medium
Likelihood: *Medium*	🟠 High	🟡 Medium	🟢 Low
Likelihood: *Low*	🟡 Medium	🟢 Low	🟢 Low

Impact

High Significant loss of assets in the protocol, significant harm to a group of users, or a core functionality of the protocol is disrupted.

Medium A small amount of funds can be lost or ancillary functionality of the protocol is affected. The user or protocol may experience reduced or delayed receipt of intended funds.

Low Can lead to any unexpected behavior with some of the protocol's functionalities that is notable but does not meet the criteria for a higher severity.

Likelihood

High The attack is possible with reasonable assumptions that mimic on-chain conditions, and the cost of the attack is relatively low compared to the amount gained or the disruption to the protocol.

Medium An attack vector that is only possible in uncommon cases or requires a large amount of capital to exercise relative to the amount gained or the disruption to the protocol.

Low Unlikely to ever occur in production.

Audit Scope & Methodology

Methodology

Guardian is the ultimate standard for Smart Contract security. An engagement with Guardian entails the following:

- Two competing teams of Guardian security researchers performing an independent review.
- A dedicated fuzzing engineer to construct a comprehensive stateful fuzzing suite for the project.
- An engagement lead security researcher coordinating the 2 teams, performing their own analysis, relaying findings to the client, and orchestrating the testing/verification efforts.

The auditing process pays special attention to the following considerations:

- Testing the smart contracts against both common and uncommon attack vectors.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross-referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts. Comprehensive written tests as a part of a code coverage testing suite.
- Contract fuzzing for increased attack resilience.

Findings & Resolutions

ID	Title	Category	Severity	Status
L-01	Unexpected Lock End Date	Unexpected Behavior	Low	Resolved
L-02	timeLockEnds Optimization	Optimization	Low	Resolved
L-03	No Requirement To Lock For The Lock Period	Unexpected Behavior	Low	Acknowledged
L-04	Lacking Event Emission	Events	Low	Resolved
L-05	Additional SNX Trapped For 2 Years	Warning	Low	Acknowledged

L-01 | Unexpected Lock End Date

Category	Severity	Location	Status
Unexpected Behavior	Low	TLXConversion.sol: 75	Resolved

Description

In the constructor for the `TLXConversion` contract the `timeLockEnds` is assigned to the `VESTING_START_TIME` + 30 days.

It was mentioned that the lock end date is expected to be January 5th, but since December has 31 days the lock end date is instead January 4th.

vesting start time: 1733356800
30 days: 2592000
end timestamp: 1735948800 (Jan. 4th 12 AM GMT)

Recommendation

Consider if this is the expected lock end date, if it is then no changes are necessary. If the lock end date must be January 5th then update the `VESTING_LOCK_DURATION` to 31 days.

Resolution

Synthetix Team: The issue was resolved in commit 25c65e7.

L-02 | timeLockEnds Optimization

Category	Severity	Location	Status
Optimization	Low	TLXConversion.sol: 84	Resolved

Description

In the `vestableAmount` function there is an early return case for `block.timestamp < timeLockEnds`, however if the `block.timestamp` is equal to the `timeLockEnds` time then the early return of 0 vested amount can apply as well.

Recommendation

Consider updating the early return case to include `block.timestamp <= timeLockEnds`.

Resolution

Synthetix Team: The issue was resolved in commit 7cf2092.

L-03 | No Requirement To Lock For The Lock Period

Category	Severity	Location	Status
Unexpected Behavior	Low	TLXConversion.sol	Acknowledged

Description

In the `TLXConversion` contract there is no requirement that users `lockAndConvert` their funds and wait for the full locking period of 30 days. A user may lock their TLX the day before the lock period ends and only have to lock their funds for a single day.

Recommendation

It is unclear if this is the expected behavior. If it is not, consider tracking locked period per account and require all accounts to wait for a 30 day lock period.

Resolution

Synthetix Team: finding is intended behavior.

L-04 | Lacking Event Emission

Category	Severity	Location	Status
Events	Low	TlxConversion.sol: 140	Resolved

Description

In the `withdrawSNX` there is no event emitted to indicate that the SNX treasury has withdrawn the remaining SNX tokens from the vester contract.

Recommendation

Consider adding an event emission to indicate that the remaining SNX tokens have been withdrawn.

Resolution

Synthetix Team: The issue was resolved in commit 8d37f14.

L-05 | Additional SNX Trapped For 2 Years

Category	Severity	Location	Status
Warning	Low	TlxConversion.sol	Acknowledged

Description

In the `TlxConversion` contract the SNX balance of the contract may not be withdrawn for 2 years after the unlock date. This includes any SNX tokens that may have been accidentally sent to the `TlxConversion` contract in excess of the amount which should be vested.

Recommendation

Consider determining the exact amount of SNX required for the TLX vest and allowing any additional SNX balance in excess of the total SNX required minus the amount claimed thus far to be re-claimed by the SNX treasury at any time.

Resolution

Synthetix Team: Acknowledged.

Disclaimer

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 Guardian 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. Guardian’s position is that each company and individual are responsible for their own due diligence and continuous security. Guardian’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 Guardian 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.

Notice that smart contracts deployed on the blockchain are not resistant from internal/external exploit. Notice that active smart contract owner privileges constitute an elevated impact to any smart contract’s safety and security. Therefore, Guardian does not guarantee the explicit security of the audited smart contract, regardless of the verdict.

About Guardian Audits

Founded in 2022 by DeFi experts, Guardian Audits is a leading audit firm in the DeFi smart contract space. With every audit report, Guardian Audits upholds best-in-class security while achieving our mission to relentlessly secure DeFi.

To learn more, visit https://guardianaudits.com

To view our audit portfolio, visit https://github.com/guardianaudits

To book an audit, message https://t.me/guardianaudits