// Security Assessment

04.22.2025 - 05.06.2025

USX Program

Solstice Labs

HALBORN

USX Program - Solstice Labs

Prepared by: HALBORN

Last Updated 06/13/2025

Date of Engagement: April 22nd, 2025 - May 6th, 2025

Summary

100% OF ALL REPORTED FINDINGS HAVE BEEN ADDRESSED

ALL FINDINGS	CRITICAL	HIGH	MEDIUM	LOW	INFORMATIONAL
11	0	0	1	5	5

TABLE OF CONTENTS

1. INTRODUCTION

The `Solstice Labs team` engaged `Halborn` to conduct a security assessment of their **USX Mint/Redeem Solana program** beginning on April 22, 2025, and ending on May 6, 2025. The security assessment was scoped to the Solana Programs provided in the usx-program GitHub repository. Commit hashes and additional details can be found in the Scope section of this report.

The `USX` Program enables authorized users to mint and redeem the USX stablecoin (referred to as `Redeemable`) in exchange for a `Collateral` token. It supports multiple types of collateral and follows a two-step process for both minting and redeeming : request and confirmation.

To mint USX, a user deposits collateral into an escrow account during the request phase. In the confirmation step, the collateral is transferred to a program-owned token account, and the corresponding amount of USX is minted to the user's wallet.

The redeem process works similarly in reverse. The user sends USX to an escrow account in the request phase. During confirmation, the USX is burned, and the equivalent collateral is returned to the user's wallet.

The program also includes instructions for managing authorizations, configurations, collateral types, and funds.

The `Solstice Labs team` further provided a code base update `eb74ce` that introduces new instructions for initializing and editing token metadata as well as addressing scenarios where users redeem amounts exceeding their initial deposits.

2. ASSESSMENT SUMMARY

`Halborn` was provided 2 weeks for the engagement and assigned one full-time security engineer to review the security of the Solana Programs in scope. The engineer is a blockchain and smart contract security expert with advanced smart contract hacking skills, and deep knowledge of multiple blockchain protocols.

The purpose of the assessment is to:

- Identify potential security vulnerabilities in the Solana Program.
- Verify the correct use of the price oracle.
- Ensure that instruction access controls are properly implemented.
- Detect any arithmetic or rounding errors.
- Confirm that the smart contract behaves as intended and aligns with the provided documentation.
- Evaluate the program's efficiency.

In summary, Halborn identified some improvements to reduce the likelihood and impact of risks, which were mostly addressed by the `Solstice Labs team` . The main ones were the following:

- `Make sure that the program rounds results in favor of the protocol.`
- `Use stored bump values for PDA derivation.`
- `Implement slippage protection .`
- `Replace floatingpoint arithmetic by integer arithmetic.`
- `Review account mutability constraints.`
- `Remove unused instruction accounts.`

4. FINDINGS OVERVIEW

SECURITY ANALYSIS	RISK LEVEL	REMEDIATION
INCORRECT ROUNDING MAY ALLOW EXCESS TOKEN MINTING	MEDIUM	SOLVED - 05/19/2025
UNUSED TRANSACTION ACCOUNT	LOW	SOLVED - 05/19/2025
UNUSED BUMP VALUES WASTE RESOURCES DURING PDA DERIVATION	LOW	SOLVED - 05/19/2025
MISSING SLIPPAGE PROTECTION ALLOWS EXECUTION AT UNFAVORABLE RATES	LOW	SOLVED - 05/19/2025
FLOATING POINT ARITHMETIC WASTES RESOURCES AND MAY INTRODUCE PRECISION LOSS	LOW	SOLVED - 05/19/2025
ACCOUNTS DO NOT NEED TO BE MUTABLE	LOW	SOLVED - 05/19/2025
RISK OF INCORRECT USERREDEEMESCROW ACCOUNT SPACE CALCULATION	INFORMATIONAL	SOLVED - 05/19/2025
INCONSISTENT DOCUMENTATION	INFORMATIONAL	SOLVED - 05/15/2025
ANYONE CAN INITIALIZE THE PROGRAM	INFORMATIONAL	ACKNOWLEDGED - 05/15/2025
PROGRAM AUTHORITY CANNOT BE CHANGED	INFORMATIONAL	FUTURE RELEASE - 05/15/2025

SECURITY ANALYSIS	RISK LEVEL	REMEDIATION
UNSUPPORTED MACRO ATTRIBUTE MAY PREVENT ANCHOR FRAMEWORK UPGRADE	INFORMATIONAL	SOLVED - 05/19/2025

Halborn strongly recommends conducting a follow-up assessment of the project either within six months or immediately following any material changes to the codebase, whichever comes first. This approach is crucial for maintaining the project's integrity and addressing potential vulnerabilities introduced by code modifications.

// Security Assessment

04.17.2025 - 04.24.2025

YieldVault

Solstice Labs

HALBORN

YieldVault - Solstice Labs

Prepared by: HALBORN

Last Updated 05/16/2025

Date of Engagement: April 17th, 2025 - April 24th, 2025

Summary

100% ⓘ OF ALL REPORTED FINDINGS HAVE BEEN ADDRESSED

ALL FINDINGS	CRITICAL	HIGH	MEDIUM	LOW	INFORMATIONAL
5	0	0	1	1	3

TABLE OF CONTENTS

1. Introduction

`Solstice Labs` engaged `Halborn` to conduct a security assessment on their **USX YieldVault Solana programs** beginning on April 17th, 2025, and ending on April 24th, 2025. The security assessment was scoped to the Solana Programs provided in usx-staking GitHub repository. Commit hashes and further details can be found in the Scope section of this report.

The `USX Yield Vault Program` enables users to lock their USX stablecoin in exchange for eUSX tokens, which represent their share in the vault. As the vault earns rewards in USX over time, the value of eUSX increases. Users can redeem their asset at any point by burning eUSX to receive their original USX deposit along with a proportional share of the accumulated rewards. This mechanism provides a simple and secure way to earn passive yield on USX holdings.

Note: During our assessment, the Solstice Labs team renamed several parts of the codebase, primarily variables and function names. As a result, some remediation references may not match the code in the commit hash that was in scope for the assessment. These differences are due to renaming and should be taken into account when reviewing the findings. The report reflects the updated naming for consistency. However, the original commit used for the assessment (and referenced in the report) may still contain the earlier names. These renaming were reviewed thoroughly and do not introduce any additional security risks.

2. Assessment Summary

`Halborn` was provided 8 days for the engagement and assigned one full-time security engineer to review the security of the Solana Programs in scope. The engineer is a blockchain and smart contract security expert with advanced smart contract hacking skills, and deep knowledge of multiple blockchain protocols.

The purpose of the assessment is to:

- Identify potential security issues within the Solana Programs.
- Ensure that smart contract functionality operates as intended.

In summary, Halborn identified some improvements to reduce the likelihood and impact of risks, which were mostly addressed by the `Solstice Labs team`. The main ones were the following:

- `Implement a check to prevent zero share minting in lock instruction.`
- `Only compute additional_lamports if the current share_mint balance is below the required minimum.`
- `Validate asset_mint to be the official USX mint.`
- `Implement a mechanism to transfer authority.`

Out-of-Scope: Third party dependencies and economic attacks.

REMEDIATION COMMIT ID:

- 26bc7a6
- 181bde9
- https://github.com/Solstice-Labs-Official/usx-staking/tree/000d10d937a0b1a439176d7211e21a83606b1981

Out-of-Scope: New features/implementations after the remediation commit IDs.

4. FINDINGS OVERVIEW

SECURITY ANALYSIS	RISK LEVEL	REMEDIATION
INCORRECT CALCULATION OF ADDITIONAL_LAMPORTS LEADS TO PREVENTION OF TOKEN METADATA INSTRUCTIONS	MEDIUM	SOLVED - 05/14/2025
LOSS OF USX DEPOSIT DUE TO ZERO SHARE MINTS	LOW	SOLVED - 05/06/2025
THE USX MINT IS NOT VALIDATED DURING YIELD POOL INITIALIZATION	INFORMATIONAL	SOLVED - 05/06/2025
AUTHORITY TRANSFER FUNCTIONALITY NOT IMPLEMENTED	INFORMATIONAL	SOLVED - 05/06/2025
RISK OF FRONT-RUNNING DURING PROGRAM INITIALIZATION	INFORMATIONAL	ACKNOWLEDGED - 05/11/2025

Halborn strongly recommends conducting a follow-up assessment of the project either within six months or immediately following any material changes to the codebase, whichever comes first. This approach is crucial for maintaining the project's integrity and addressing potential vulnerabilities introduced by code modifications.

// Security Assessment

04.24.2025 - 04.28.2025

Rewarder SCA

Solstice Labs

HALBORN

Rewarder SCA - Solstice Labs

Prepared by: HALBORN

Last Updated 05/23/2025

Date of Engagement: April 24th, 2025 - April 28th, 2025

Summary

100% OF ALL REPORTED FINDINGS HAVE BEEN ADDRESSED

ALL FINDINGS	CRITICAL	HIGH	MEDIUM	LOW	INFORMATIONAL
2	0	0	0	0	2

TABLE OF CONTENTS

1. Introduction

`Solstice Labs` engaged `Halborn` to conduct a security assessment on their **USX Staking Solana programs** beginning on April 24th, 2025, and ending on April 28th, 2025. The security assessment was scoped to the Solana Programs provided in usx-rewarder GitHub repository. Commit hashes and further details can be found in the Scope section of this report.

Note: During our assessment, the Solstice Labs team renamed several parts of the codebase, primarily variables and function names. As a result, some remediation references may not match the code in the commit hash that was in scope for the assessment. These differences are due to renaming and should be taken into account when reviewing the findings. The report reflects the updated naming for consistency. However, the original commit used for the assessment (and referenced in the report) may still contain the earlier names. These renaming were reviewed thoroughly and do not introduce any additional security risks.

2. Assessment Summary

`Halborn` was provided 3 days for the engagement and assigned one full-time security engineer to review the security of the Solana Programs in scope. The engineer is a blockchain and smart contract security expert with advanced smart contract hacking skills, and deep knowledge of multiple blockchain protocols.

The purpose of the assessment is to:

- Identify potential security issues within the Solana Programs.
- Ensure that smart contract functionality operates as intended.

In summary, `Halborn` identified some improvements to reduce the likelihood and impact of risks, which have been addressed by Solstice Labs team. The main ones were the following:

- `Validate asset_mint to be the official USX mint.`

SECURITY ANALYSIS	RISK LEVEL	REMEDIATION
THE USX MINT IS NOT VALIDATED DURING CONTROLLER INITIALIZATION	INFORMATIONAL	SOLVED - 05/05/2025
RISK OF FRONT-RUNNING DURING PROGRAM INITIALIZATION	INFORMATIONAL	ACKNOWLEDGED - 05/20/2025

Halborn strongly recommends conducting a follow-up assessment of the project either within six months or immediately following any material changes to the codebase, whichever comes first. This approach is crucial for maintaining the project's integrity and addressing potential vulnerabilities introduced by code modifications.