October 5th, 2023

DexHunter - Stop Loss

TxPipe Shop

Contents

1 - Summary

We undertook a thorough examination of DexHunter's Stop Loss validator. DexHunter, a decentralized exchange (DEX) aggregator, emphasizes a high quality user interface (UI) and user experience (UX), orchestrating a suite of features to enhance liquidity provision and order execution. These features include:

- Swaps orchestration across six distinct DEX platforms
- Token baskets provision for diversified asset exposure
- Standard limit orders facilitation
- Split limit order execution into up to 40 segmented parts

The audit is conducted without warranties or guarantees of the quality or security of the code. The investigation spanned several potential vulnerabilities, including scenarios where attackers might exploit the validator to lock up or steal funds. It's important to note that this report only covers identified issues, and we do not claim to have detected all potential vulnerabilities.

1.a - Overview

DexHunter endeavors to extend their capabilities by executing stop loss orders without necessitating the interim holding of ADA (Cardano's native token) by the DexHunter team. The conventional limit order functionality is perceived as insufficient for this purpose since such orders, once placed, would merely get executed, hence not serving the stop loss function. The Stop Loss validator is engineered to harbor pre-created user orders, which are subsequently submitted to the various DEXs by a designated backend, acting on behalf of the user.

The process of instigating a stop loss order is streamlined, necessitating merely the transfer of assets along with a datum to the validator's address. The validator is programmed to undertake two critical actions when checking whether an order UTXO (Unspent Transaction Output) can be spent, namely: cancel and execute.

- **Cancel Action**: In a cancel operation, the validator scrutinizes the transaction to ensure it is authenticated by the signature of the owner, as specified in the datum.
- **Execute Action**: In an execution scenario, the validator extends its validation to ascertain the integrity of the order and verifies that the transaction is authenticated by the backend's signature, again as dictated by the datum.

This architecture endows users with a robust mechanism to place stop loss orders, enhancing their trading strategy while maintaining a trustless ethos by obviating the need for an intermediary to hold ADA.

1.b - Process

The audit process involved a meticulous review of the stop loss contract for the DexHunter platform. Our team focused on scrutinizing areas susceptible to potential security threats, where attackers could exploit the contract's functions to lock up or steal funds from the dApp and its users. Our methodical approach encompassed a range of potential attack vectors, including unauthorized minting, funds theft, denial of service, and business requirements violation, among others. The audit, carried out from Oct 1 to Oct 5, 2023, involved regular interactions on Discord where feedback was submitted. The DexHunter addressed all issues, as detailed in this report.

1.b.a - Files Audited

Below is a list of all files audited in this report, any files **not** listed here were **not** audited. The final state of the files for the purposes of this report is considered to be commit `dd2eacc8c173c4f25e56d8545c9719d314c1f60a`.

Filename
validators/stoploss.ak

2 - Findings

ID	Title	Severity	Status
DH-001	Double Satisfaction with multiple datums	Critical	Resolved
DH-002	Backend can add extra tokens in the stop loss outputs	Critical	Resolved
DH-301	Interoperability with other validators	Info	Resolved
DH-302	Faster output validation	Info	Resolved

3 - DH-001 Double Satisfaction with multiple datums

Category	Commit	Severity	Status
Exploit	a7f6fffcd8d01ab0ccb6ce6275fd3d5662afd7df	Critical	Resolved

3.a - Description

A transaction that spends multiple datums with the same or similar stop loss outputs could use one of the datums outputs to satisfy the output conditions for multiple datums which would allow for the theft of funds from the other datums.

3.b - Recommendation

For each transactions spending a datum, it should expect an output with a unique datum. Following output is the stop loss outputs specified by the datum. By having this unique output first for each datum spent, it would prevent multiple datums from being satisfied by a single set of outputs.

3.c - Resolution

Resolved in commit `b6f4d6e1b909e4592cc9604b9d04c4b65dee32cf`

4 - DH-002 Backend can add extra tokens in the stop loss outputs

Category	Commit	Severity	Status
Exploit	a7f6fffcd8d01ab0ccb6ce6275fd3d5662afd7df	Critical	Resolved

4.a - Description

A backend could add extra tokens to the stop loss outputs. This would allow the backend to create outputs that are locked permanently and unable to be picked up by the dex batcher.

4.b - Recommendation

Add a check that the stop loss outputs are only the token specified in the datum and lovelace.

4.c - Resolution

Resolved in commit `56b7ef63032e590af506b9064b74fdff86663e84`

5 - DH-301 Interoperability with other validators

Category	Commit	Severity	Status
Enhancement	a7f6fffcd8d01ab0ccb6ce6275fd3d5662afd7df	Info	Resolved

5.a - Description

Adding the ability to use NFTs as ownership credentials paves the way for future interoperibility with other validators.

5.b - Recommendation

Allow the owner of a datum to be an NFT or a public key.

5.c - Resolution

Resolved in commit `b6f4d6e1b909e4592cc9604b9d04c4b65dee32cf`

6 - DH-302 Faster output validation

Category	Commit	Severity	Status
Optimization	a7f6fffcd8d01ab0ccb6ce6275fd3d5662afd7df	Info	Resolved

6.a - Description

The current method of validating the outputs starts from the first output and cycles through the list until an output is found matching the conditions. Then the next output to be validated starts from the beginning and searches the whole list again.

6.b - Recommendation

Rather than searching blindly through the whole list. You can expect a juxtaposed ordering on the outputs to validate. Then each output can be validated in order. Outputs not in order would simply be invalid transactions. This would reduce the time complexity from O(n*k) to O(k).

6.c - Resolution

Resolved in commit `b6f4d6e1b909e4592cc9604b9d04c4b65dee32cf`

7 - Appendix

7.a - Disclaimer

This report is governed by the terms in the agreement between TxPipe (**TXPIPE**) and DEX Hunter (**CLIENT**). This report cannot be shared, referred to, altered, or relied upon by any third party without TXPIP's written consent. This report does not endorse or disapprove any specific project, team, code, technology, asset or similar. It provides no warranty or guarantee about the quality or nature of the technology analyzed.

TXPIPE DISCLAIMS ALL WARRANTIES, EXPRESSED OR IMPLIED, related to this report, its content, and the related services and products. This report is provided as-is. TxPipe does not take responsibility for any product or service advertised or offered by Client or any third party. **TXPIPE IS NOT RESPONSIBLE FOR MONITORING ANY TRANSACTION BETWEEN YOU AND CLIENT AND/OR ANY THIRD-PARTY PROVIDERS OF PRODUCTS OR SERVICES.**

This report should not be used for making investment or involvement decisions with any project, services or assets. This report provides general information and is not a form of financial, investment, tax, legal, regulatory, or other advice.

TxPipe created this report as an informational review of the due diligence performed on the Client's smart contract. This report provides no guarantee on the security or operation of the smart contract on deployment or post-deployment. **TXPIPE HAS NO DUTY TO MONITOR CLIENT'S OPERATION OF THE PROJECT AND UPDATE THE REPORT ACCORDINGLY.**

The information in this report may not cover all vulnerabilities. This report represents an extensive assessment process intended to help increase the quality of the Client's code. However, blockchain technology and cryptographic assets present a high level of ongoing risk, including unknown risks and flaws.

TxPipe recommends multiple independent audits, a public bug bounty program, and continuous security auditing and monitoring. Errors in the manual review process are possible, and TxPipe advises seeking multiple independent opinions on critical claims. **TXPIPE BELIEVES EACH COMPANY AND INDIVIDUAL IS RESPONSIBLE FOR THEIR OWN DUE DILIGENCE AND CONTINUOUS SECURITY.**

7.b - Issue Guide

7.b.a - Severity

Severity	Description
Critical	Critical issues highlight exploits, bugs, loss of funds, or other vulnerabilities that prevent the dApp from working as intended. These issues have no workaround.
Major	Major issues highlight exploits, bugs, or other vulnerabilities that cause unexpected transaction failures or may be used to trick general users of the dApp. dApps with Major issues may still be functional.
Minor	Minor issues highlight edge cases where a user can purposefully use the dApp in a non-incentivized way and often lead to a disadvantage for the user.
Info	Info are not issues. These are just pieces of information that are beneficial to the dApp creator. These are not necessarily acted on or have a resolution, they are logged for the completeness of the audit.

7.b.b - Status

Status	Description
Resolved	Issues that have been **fixed** by the **project** team.
Acknowledged	Issues that have been **acknowledged** or **partially fixed** by the **project** team. Projects can decide to not **fix** issues for whatever reason.
Identified	Issues that have been **identified** by the **audit** team. These are waiting for a response from the **project** team.

7.c - Revisions

This report was created using a git based workflow. All changes are tracked in a github repo and the report is produced using typst. The report source is available here. All versions with downloadable PDFs can be found on the releases page.

7.d - About Us

TxPipe is a blockchain technology company responsible for many projects that are now a critical part of the Cardano ecosystem. Our team built Oura, Scrolls, Pallas, Demeter, and we're the original home of Aiken. We're passionate about making tools that make it easier to build on Cardano. We believe that blockchain adoption can be accelerated by improving developer experience. We develop blockchain tools, leveraging the open-source community and its methodologies.

7.d.a - Links

- Website
- Email
- Twitter