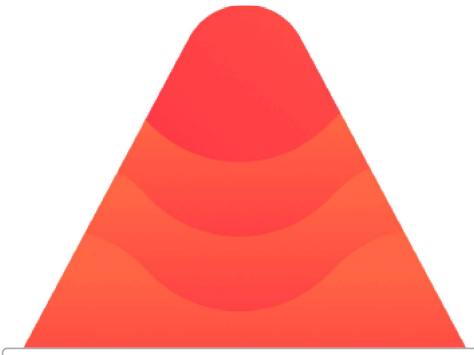
(https://blog.coinfabrik.com/)

SMART CONTRACT AUDIT (HTTPS://BLOG.COINFABRIK.COM/CATEGORY/SMART-CONTRACTS/SMART-CONTRACT-AUDIT-SMART-CONTRACTS/)

Avalaunch Audit <> Allocation Staking and Cooldown feature

Heloisa Ceni (https://blog.coinfabrik.com/author/heloisa-ceni/)

December 16, 2021 (https://blog.coinfabrik.com/smart-contracts/avalaunch-audit-allocation-staking-and-cooldown-feature/)



Contents

Introduction

CoinFabrik was asked to audit the contracts for the Avalaunch AllocationStaking project. First we will provide a summary of our discoveries and then we will show the details of our findings.

Summary

The contracts audited are from the GitHub repository at https://github.com/avalaunch-app/xava-protocol.

The audit is based on the commit fc32d84a67233ebba6f980182a951076858d30c0.

Contracts

The audited contracts are:

- contracts/AllocationStaking.sol
- contracts/sales/AvalaunchSale.sol
- contracts/sales/SalesFactory.sol

Analyses

The following analyses were performed:

- Misuse of the different call methods
- Integer overflow errors
- Division by zero errors
- Outdated version of Solidity compiler
- Front running attacks
- Reentrancy attacks
- Misuse of block timestamps
- Softlock denial of service attacks
- Functions with excessive gas cost
- Missing or misused function qualifiers
- Needlessly complex code and contract interactions
- Poor or nonexistent error handling
- Failure to use a withdrawal pattern
- Insufficient validation of the input parameters
- Incorrect handling of cryptographic signatures

Findings and Fixes

ID	Title	Severity	Status
MI-01	Failure to Use safeMath Library	Minor	Not fixed
EN-01	Unvalidated Input in Function and Constructor	Enhancement	Not fixed

Severity Classification

Security risks are classified as follows:

- **Critical**: These are issues that we manage to exploit. They compromise the system seriously. They must be fixed immediately.
- **Medium:** These are potentially exploitable issues. Even though we did not manage to exploit them or their impact is not clear, they might represent a security risk in the near future. We suggest fixing them as soon as possible.
- **Minor:** These issues represent problems that are relatively small or difficult to take advantage of but can be exploited in combination with other issues. These kinds of issues do not block deployments in production environments. They should be taken into account and be fixed when possible.
- **Enhancement:** These kinds of findings do not represent a security risk. They are best practices that we suggest to implement.

This classification is summarized in the following table:

SEVERITY	EXPLOITABLE	ROADBLOCK	TO BE FIXED
Critical	Yes	Yes	Immediately
Medium	In the near future	Yes	As soon as possible
Minor	Unlikely	No	Eventually
Enhancement	No	No	Eventually

Issues Found by Severity

Critical Severity Issues

No issues found.

Medium Severity Issues

No issues found.

Minor Severity Issues

MI-01 Failure to Use safeMath Library

The functions `fund() (line 120)`, `totalPending() (line 196)` and `erc20Transfer() (line 412)` make use of standard arithmetic which are susceptible to overflows and underflows.

Recommendation

Replace + by `add()` and – by `sub()`.

Enhancements

EN-01 Unvalidated Input in Function and Constructor

The following are functions and constructors that fail to validate the input. In most cases, they are used to set parameters which may be changed later and the impact of setting a bad parameter is small.

- The parameter _token in `setSaleParams()` is not checked to be non-null.
- The input `addresses _erc20` and `_salesFactory` in the AllocationStaking constructor are not checked to be non-null.

Conclusion

We found the contracts to be simple and straightforward and have an adequate amount of documentation. A minor vulnerability pointing to unsafe use of math was found in some functions with little security impact.

Disclaimer: This audit report is not a security warranty, investment advice, or an approval of the Avalaunch project since CoinFabrik has not reviewed its platform. Moreover, it does not provide a smart contract code faultlessness guarantee.

Related Posts

(https://blog.coinfabrik.com/smart-contracts/smart-contract-audit-smart-contracts/avalaunch-audit-allocation-staking-and-sales/)

Avalaunch Audit <>Allocation Staking and Sales (https://blog.coinfabrik.com/smart-contracts/smart-contract-audit-smart-contracts/avalaunch-audit-allocation-staking-and-sales/)

Introduction CoinFabrik was asked to audit the contracts for the Avalaunch project. First we will…

(https://blog.coinfabrik.com/uncategorized/blox-staking-audit-vesting-and-dex-contracts/)

BLOX STAKING Audit: Vesting and DEX Contracts (https://blog.coinfabrik.com/uncategorized/blox-staking-audit-vesting-and-dex-contracts/)

Introduction CoinFabrik was asked to audit the contracts for the Vesting for Blox Staking. First…

(https://blog.coinfabrik.com/smart-contracts/smart-contract-audit-smart-contracts/katana-

Katana Smart Contract Audit (https://blog.coinfabrik.com/smart-contracts/smart-contract-audit-smart-contracts/katana-smart-contract-audit/)

CoinFabrik was asked to audit the contracts for the Katana project. First we will

katana-

smart-

contract-

audit/)

(https://blog.coinfabrik.com/smart-

contract-

audit/bit2me-

token-

security-

audit/)

Bit2Me Token - Security Audit

(https://blog.coinfabrik.com/smart-contract-audit/bit2me-token-security-audit/)

Introduction CoinFabrik was asked to audit the contracts for the Bit2Me project.

First, we will...

Tags:

#avalaunch #smartcontract #audit (https://blog.coinfabrik.com/tag/avalaunch-smartcontract-audit/)

#coinfabrik (https://blog.coinfabrik.com/tag/coinfabrik/)

#smartcontract (https://blog.coinfabrik.com/tag/smartcontract/)

#smartcontractaudit (https://blog.coinfabrik.com/tag/smartcontractaudit/)

SHARE ON

(https://www.facebook.com/sharer/sharer.php?u=https://blog.coinfabrik.com/smart-contracts/a

(https://twitter.com/intent/tweet?text=Avalaunch%20Audit%20%20Allocation%20Staking%20and%20%20%20%20%20%20%20%20contracts/avalaunch-audit-allocation-staking-and-cooldown-feature/)

(https://pinterest.com/pin/create/button/?url=&media=https://blog.coinfabrik.com/wp-content/u logo.png&description=Avalaunch+Audit+%3C%3E+Allocation+Staking+and++++++++++++Cooldo

(https://www.linkedin.com/shareArticle?mini=true&url=https://blog.coinfabrik.com/smart-contrac feature/&title=Avalaunch%20Audit%20%20Allocation%20Staking%20and%20%20%20%20%20%20

← PREVIOUS ARTICLE

AlexGo Audit (https://blog.coinfabrik.com/smart-contracts/alexgo-audit/)

NEXT ARTICLE →

EMDX – Protocol Audit (https://blog.coinfabrik.com/smart-contracts/smart-contract-audit-smart-contracts/emdx-protocol-audit/)

You may also like

(https://blog.coinfabrik.com/smart-contracts/magic-bridge-audit/)

Magic Bridge Audit (https://blog.coinfabrik.com/smart-contracts/magic-bridge-audit/)

(https://blog.coinfabrik.com/smart-contracts/smart-contract-audit-smart-contracts/mintingfactoryv2-baseupgradablemarketplace-kodav3upgradablegatedmarketplace/)

2 months ago | Smart Contract Audit (https://blog.coinfabrik.com/category/smart-contracts/smart-contract-audit-smart-contracts/)

MintingFactoryV2, BaseUpgradableMarketplace & KODAV3UpgradableGatedMarketplace (https://blog.coinfabrik.com/smart-contracts/smart-contract-audit-smart-contracts/mintingfactoryv2-baseupgradablemarketplace-kodav3upgradablegatedmarketplace/)