// Private Solana Program Security Assessment 07.29.2024 - 08.05.2024

Staking Program

IO.NET

HALBORN

Staking Program - IO.NET

Prepared by: HALBORN

Last Updated 08/20/2024

Date of Engagement by: July 29th, 2024 - August 5th, 2024

Summary

100% ⓘ OF ALL REPORTED FINDINGS HAVE BEEN ADDRESSED

ALL FINDINGS	CRITICAL	HIGH	MEDIUM	LOW	INFORMATIONAL
9	4	0	0	3	2

TABLE OF CONTENTS

1. Introduction

IO.NET engaged Halborn to conduct a security assessment on their **Staking Solana program** beginning on July 29th, 2024 and ending on Aug 5th, 2024. The security assessment was scoped to the Solana Programs provided in their io-staking-contract GitHub repository. Commit hashes and further details can be found in the Scope section of this report.

The **io staking contract** is a staking platform built on the Solana blockchain using the Anchor framework. It allows users to stake tokens, earn rewards, and withdraw their stakes. The contract also includes functionality for initializing Merkle roots, which are used for secure reward distribution.

2. Assessment Summary

Halborn was provided 1 week 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 security concerns, that have been addressed by the IO.NET team. The main ones were the following:

- Global Vault Token Account can be drained
- Deposit can be front-run
- Access Control validation missing may lead to denial Of Service
- Unauthorized withdrawal from other users' already unstaked accounts.

3. SCOPE

FILES AND REPOSITORY

(a) Repository: io-staking-contract

(b) Assessed Commit ID: 90bd801

(c) Items in scope:

- programs/staking/src/error.rs
- programs/staking/src/lib.rs
- programs/staking/src/state.rs
- programs/staking/src/event.rs
- programs/staking/src/instructions/claim.rs
- programs/staking/src/instructions/deposit.rs
- programs/staking/src/instructions/initialize.rs
- programs/staking/src/instructions/merkle_tree.rs
- programs/staking/src/instructions/mod.rs
- programs/staking/src/instructions/reward.rs
- programs/staking/src/instructions/stake.rs
- programs/staking/src/instructions/unstake.rs
- programs/staking/src/instructions/withdraw.rs
- programs/staking/src/instructions/set_authority.rs
- ionet-official/io-staking-contract/commit/02568dd734b2afc27b00392e08966692d1f0ac75

Out-of-Scope:

REMEDIATION COMMIT ID:

- c920694
- e4673dc
- 5e28eb5
- ddb27ab
- 1980d75
- da56012
- e3446d9

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

4. FINDINGS OVERVIEW

SECURITY ANALYSIS	RISK LEVEL	REMEDIATION
DEPOSIT MAY BE FRONT-RUN	CRITICAL	SOLVED - 08/06/2024
ACCESS CONTROL VALIDATION MISSING MAY LEAD TO DENIAL OF SERVICE	CRITICAL	SOLVED - 08/08/2024
GLOBAL VAULT TOKEN ACCOUNT CAN BE DRAINED	CRITICAL	SOLVED - 08/08/2024
UNAUTHORIZED WITHDRAWAL FROM OTHER USERS' ALREADY UNSTAKED ACCOUNTS	CRITICAL	SOLVED - 08/02/2024
STAKE INSTRUCTION RESULTS IN STACK OVERFLOW	LOW	SOLVED - 08/06/2024
NEW AUTHORITY CHECK MISSING	LOW	RISK ACCEPTED
UNSTAKE FROM DIFFERENT POOL MAY LEAD TO INCONSISTENCY AND OVERFLOW	LOW	SOLVED - 08/07/2024
MULTIPLE TOKEN ACCOUNTS CHECK MISSING	INFORMATIONAL	SOLVED - 08/08/2024
REDUNDANT ACCOUNTS AND DATA	INFORMATIONAL	SOLVED - 08/08/2024

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.