KUDELSKI SECURITY

Solrazr Security Assessment

Summary Report

Findings and Recommendations Report Presented to:

Solrazr

September 03, 2021
Version: 1.0 Final

Presented by:

Kudelski Security, Inc.
5090 North 40th Street, Suite 450
Phoenix, Arizona 85018

For Public Release

EXECUTIVE SUMMARY

Overview

Solrazr, a decentralized developer ecosystem for Solana, engaged Kudelski Security to perform a security review of their product prior to launch. This assessment took place from August 2 to August 18, 2021, and focused on the following objectives:

- Provide the customer with an assessment of their overall security posture and any risks that were discovered within the environment during the engagement
- To provide a professional opinion on the maturity, adequacy, and efficiency of the security measures that are in place
- To identify potential issues with the codebase and include improvement recommendations based on the result of our tests

Following initial findings & remediation, a re-review of the Solrazr code base was conducted on September 1, 2021.

All of the High, Medium, and Low-risk vulnerabilities found have been resolved our satisfaction.

Resolved Findings

#	Severity	Status	Description
KS-SOLRAZR-F-01	High	RESOLVED	Unverified program invocation in ExecuteTokenSale allows users to steal SOLR tokens
KS-SOLRAZR-F-02	Medium	RESOLVED	CloseWhitelistAccount must zero out account data to avoid abuse
KS-SOLRAZR-F-03	Medium	RESOLVED	Insufficient verification allows DoS through SetAllocationToZero
KS-SOLRAZR-F-04	Low	RESOLVED	Linting errors indicate bad code practices (Token Sale)

During the test, the following positive observations were noted regarding the scope of the engagement:

- The team was very supportive and open to discuss the design choices made
- Architecural drawing was made available and formed the basis of the review
- The team resolved issues identified in a fast and efficient manner
- Authorization for RemoveFromWhitelist is sufficient
- Authorization for AddToWhitelist is sufficient
- Authorization for InitTokenWhitelist is sufficient

Based on the account relationship graphs or reference graphs and the formal verification we can conclude that the reviewed code implements the documented functionality and that all findings are resolved to our satisfaction.

Appendix: Scope and Rules Of Engagement

The following table documents the targets in scope for the engagement. No additional systems or resources were in scope for this assessment.

The source code was supplied through private repositories at https://github.com/solrazr-app/token-whitelist with the commit hash cd7512762231955a76acd156ae2065c79705bfe3 and https://github.com/solrazr-app/solr-token-sale with the commit hash 98b08ec5f3e3a393415410fabde702b00bf2a59b

Files included in the code review	
token-whitelist/program/ ├── Cargo.lock ├── Cargo.toml ├── src/ │ ├── entrypoint.rs │ ├── error.rs │ ├── instruction.rs │ ├── lib.rs │ ├── processor.rs │ └── state.rs └── Xargo.toml	Rust implementation of the whitelist program
solr-token-sale/program/ ├── Cargo.lock ├── Cargo.toml ├── src/ │ ├── entrypoint.rs │ ├── error.rs │ ├── instruction.rs │ ├── lib.rs │ ├── processor.rs │ └── state.rs └── Xargo.toml	Rust implementation of the token sale program

Table 1: Scope

ABOUT KUDELSKI SECURITY

Kudelski Security is an innovative, independent Swiss provider of tailored cyber and media security solutions to enterprises and public sector institutions. Our team of security experts delivers end-to-end consulting, technology, managed services, and threat intelligence to help organizations build and run successful security programs. Our global reach and cyber solutions focus is reinforced by key international partnerships.

Kudelski Security is a division of Kudelski Group. For more information, please visit https://www.kudelskisecurity.com.

Kudelski Security

route de Genève, 22-24

1033 Cheseaux-sur-Lausanne

Switzerland

Kudelski Security

5090 North 40th Street

Suite 450

Phoenix, Arizona 85018