QuillAudits

Audit Report
March, 2023

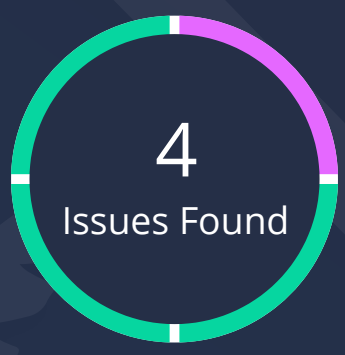
For

redefined

Table of Content

Executive Summary

Project Name	Redefined
Overview	Redefined is launching a name service aggregator offered through one SDK integration; in addition to that, redefined is launching two resolvers, one for emails and the other for usernames.
Timeline	17 March, 2023 to 29 March, 2023
Method	Manual Review, Functional Testing, Automated Testing etc.
Scope of Audit	The scope of this audit was to analyse Redefined codebase for quality, security, and correctness.
CodeBase	*https://github.com/e2xlabs/redefined-connect-decentralized/*
Branch	Main
Commit Hash	47000915d3edcd3c84bd458748997b4aaa4b9002
Fixed In Commit	25ee1ea10488d48bd712e576fab7630bab76d195



High
Medium
Low
Informational

	High	Medium	Low	Informational
Open Issues	0	0	0	0
Acknowledged Issues	0	0	0	0
Partially Resolved Issues	0	0	0	0
Resolved Issues	0	0	**3**	**1**

Types of Severities

High

A high severity issue or vulnerability means that your smart contract can be exploited. Issues on this level are critical to the smart contract's performance or functionality, and we recommend these issues be fixed before moving to a live environment.

Medium

The issues marked as medium severity usually arise because of errors and deficiencies in the smart contract code. Issues on this level could potentially bring problems, and they should still be fixed.

Low

Low-level severity issues can cause minor impact and or are just warnings that can remain unfixed for now. It would be better to fix these issues at some point in the future.

Informational

These are severity issues that indicate an improvement request, a general question, a cosmetic or documentation error, or a request for information. There is low-to-no impact.

Types of Issues

Open

Security vulnerabilities identified that must be resolved and are currently unresolved.

Resolved

These are the issues identified in the initial audit and have been successfully fixed.

Acknowledged

Vulnerabilities which have been acknowledged but are yet to be resolved.

Partially Resolved

Considerable efforts have been invested to reduce the risk/impact of the security issue, but are not completely resolved.

Checked Vulnerabilities

- Re-entrancy
- Timestamp Dependence
- Gas Limit and Loops
- Exception Disorder
- Gasless Send
- Use of tx.origin
- Compiler version not fixed
- Address hardcoded
- Divide before multiply
- Integer overflow/underflow
- Dangerous strict equalities
- Tautology or contradiction
- Return values of low-level calls
- Missing Zero Address Validation
- Private modifier
- Revert/require functions
- Using block.timestamp
- Multiple Sends
- Using SHA3
- Using suicide
- Using throw
- Using inline assembly

Techniques and Methods

Throughout the audit of smart contract, care was taken to ensure:

- The overall quality of code.
- Use of best practices.
- Code documentation and comments match logic and expected behaviour.
- Token distribution and calculations are as per the intended behaviour mentioned in the whitepaper.
- Implementation of ERC-20 token standards.
- Efficient use of gas.
- Code is safe from re-entrancy and other vulnerabilities.

The following techniques, methods and tools were used to review all the smart contracts.

Structural Analysis

In this step, we have analysed the design patterns and structure of smart contracts. A thorough check was done to ensure the smart contract is structured in a way that will not result in future problems.

Static Analysis

Static analysis of smart contracts was done to identify contract vulnerabilities. In this step, a series of automated tools are used to test the security of smart contracts.

Code Review / Manual Analysis

Manual analysis or review of code was done to identify new vulnerabilities or verify the vulnerabilities found during the static analysis. Contracts were completely manually analysed, their logic was checked and compared with the one described in the whitepaper. Besides, the results of the automated analysis were manually verified.

Gas Consumption

In this step, we have checked the behaviour of smart contracts in production. Checks were done to know how much gas gets consumed and the possibilities of optimization of code to reduce gas consumption.

Tools and Platforms used for Audit

Remix IDE, Truffle, Truffle Team, Solhint, Mythril, Slither, Solidity statistic analysis.

Manual Testing

High Severity Issues

No issues found

Medium Severity Issues

No issues found

Low Severity Issues

L.1 Inherited OwnableUpgradeable uses single-step ownership transfer

Description

During the code review, It has been noticed that the EmailNameService, NickNameService contracts use single-step ownership transfer on the OwnableUpgradeable contract.

Remediation

Consider using the *Ownable2StepUpgradable* contract in the implementation.

Status

Resolved

L.2 Remove garbage

Description

At various places in the contract hardhat/console.sol is imported.

Remediation

In general, hardhat/console.sol is used only for testing and debugging, the deployed version of the contracts should not contain that.
We recommend removing the import.

Status

Resolved

L.3 Used locked pragma version

Description

The pragma versions used in the contract are not locked. Consider using the latest versions among 0.8.19 for deploying the contracts and libraries as it does not compile for any other version and can be confusing for a developer. Solidity source files indicate the versions of the compiler they can be compiled with.

pragma solidity ^0.8.0; // bad: compiles between 0.8.0 and 0.8.19
pragma solidity 0.8.0; // good: compiles w 0.8.0 only but not the latest version
pragma solidity 0.8.19; // best: compiles w 0.8.19

Remediation

Use best compiles and locked pragma in the contracts.

Status

Resolved

Informational Issues

I.1 Recommendations and Gas optimizations

Description

1. For test stake use *smock* Library.
2. Gas optimization
    - The pre-increment operation is cheaper (about 5 GAS per iteration) so use ++i instead of i++ or i+= 1 in for loop. We recommend using pre-increment in all the for loops.
    - != 0 costs 6 less GAS compared to > 0 for unsigned integers in require statements with the optimizer enabled. We recommend using !=0 instead of > 0 in all the contracts.
    - In for loop the default value initialization to 0 should be removed from all the for loops.
    - In the EVM, there is no opcode for non-strict inequalities (>=, <=) and two operations are performed (> + =.) Consider replacing >= with the strict counterpart >. Recommend following the inequality with a strict one.
    - All the public functions which are not used internally need to be converted to external.

Status

Acknowledged

Functional Tests

Some of the tests performed are mentioned below :

NickNameService

- setPricesPerLengthInUsd checked with only owner with positive and negative case ✓
- IsVirgin checked for valid and invalid domain ✓
- Withdraw with only owner is checked for positive and negative case ✓
- Register and update functionality
  - Virgin domain and normal domain both are registered ✓
  - Duplicate should not be able to preset in the function ✓
  - Domain should be in a good range ✓
  - Domain positive and negative scenarios ✓
  - verifyRecords checks ✓
  - Update is only been controlled by owner ✓
- calcNicknamePrice
  - Correct returning of price ✓
  - Passed all require checks of verifyNicknameValue ✓
- Resolve
  - Domain positive and negative scenarios ✓

EmailNameService

- backendVerificationAddress
  - Only owner allowed to add and remove backend verify addres ✓
- Withdraw with only owner is checked for positive and negative case ✓
- IsVirgin checked for valid and invalid domain ✓

- Resolve
  - Anyone address can resolve ✓
  - Correct domain can only be resolved ✓

Automated Tests

No major issues were found. Some false positive errors were reported by the tools. All the other issues have been categorized above according to their level of severity.

```
ethsec@5188c3820a66:/code/email/contracts$ slither BnbUsdQuoteProviderStub.sol

Pragma version0.8.9 (BnbUsdQuoteProviderStub.sol#2) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6
solc-0.8.9 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity

Parameter BnbUsdQuoteProviderStub.setPrice(int256)._price (BnbUsdQuoteProviderStub.sol#8) is not in mixedCase
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions

setPrice(int256) should be declared external:
        - BnbUsdQuoteProviderStub.setPrice(int256) (BnbUsdQuoteProviderStub.sol#8-10)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#public-function-that-could-be-declared-external
BnbUsdQuoteProviderStub.sol analyzed (1 contracts with 75 detectors), 4 result(s) found
```

```
ethsec@5188c3820a66:/code/email/contracts$ slither EmailNameServiceUpdateStub_flat.sol
Compilation warnings/errors on EmailNameServiceUpdateStub_flat.sol:
Warning: SPDX license identifier not provided in source file. Before publishing, consider adding a comment containing "SPDX-License-Identifier: <SPDX-License>" to each source file. Use "SPDX-License-Identifier: UNL
ICENSED" for non-open-source code. Please see https://spdx.org for more information.
--> EmailNameServiceUpdateStub_flat.sol



OwnableUpgradeable.__gap (EmailNameServiceUpdateStub_flat.sol#584) shadows:
        - ContextUpgradeable.__gap (EmailNameServiceUpdateStub_flat.sol#441)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-variable-shadowing

AddressUpgradeable._revert(bytes,string) (EmailNameServiceUpdateStub_flat.sol#211-223) uses assembly
        - INLINE ASM (EmailNameServiceUpdateStub_flat.sol#216-219)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#assembly-usage

Different versions of Solidity is used:
        - Version used: ['^0.8.0', '^0.8.1', '^0.8.2', '^0.8.9']
        - ^0.8.1 (EmailNameServiceUpdateStub_flat.sol#9)
        - ^0.8.2 (EmailNameServiceUpdateStub_flat.sol#236)
        - ^0.8.0 (EmailNameServiceUpdateStub_flat.sol#409)
        - ^0.8.0 (EmailNameServiceUpdateStub_flat.sol#452)
        - ^0.8.0 (EmailNameServiceUpdateStub_flat.sol#494)
        - ^0.8.9 (EmailNameServiceUpdateStub_flat.sol#593)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#different-pragma-directives-are-used

AddressUpgradeable._revert(bytes,string) (EmailNameServiceUpdateStub_flat.sol#211-223) is never used and should be removed
AddressUpgradeable.functionCall(address,bytes) (EmailNameServiceUpdateStub_flat.sol#90-92) is never used and should be removed
AddressUpgradeable.functionCall(address,bytes,string) (EmailNameServiceUpdateStub_flat.sol#100-106) is never used and should be removed
AddressUpgradeable.functionCallWithValue(address,bytes,uint256) (EmailNameServiceUpdateStub_flat.sol#119-125) is never used and should be removed
AddressUpgradeable.functionCallWithValue(address,bytes,uint256,string) (EmailNameServiceUpdateStub_flat.sol#133-142) is never used and should be removed
AddressUpgradeable.functionStaticCall(address,bytes) (EmailNameServiceUpdateStub_flat.sol#150-152) is never used and should be removed
AddressUpgradeable.functionStaticCall(address,bytes,string) (EmailNameServiceUpdateStub_flat.sol#160-167) is never used and should be removed
AddressUpgradeable.isContract(address) (EmailNameServiceUpdateStub_flat.sol#41-47) is never used and should be removed
AddressUpgradeable.sendValue(address,uint256) (EmailNameServiceUpdateStub_flat.sol#65-70) is never used and should be removed
AddressUpgradeable.verifyCallResult(bool,bytes,string) (EmailNameServiceUpdateStub_flat.sol#199-209) is never used and should be removed
AddressUpgradeable.verifyCallResultFromTarget(address,bool,bytes,string) (EmailNameServiceUpdateStub_flat.sol#175-191) is never used and should be removed
ContextUpgradeable.__Context_init() (EmailNameServiceUpdateStub_flat.sol#423-424) is never used and should be removed
ContextUpgradeable.__Context_init_unchained() (EmailNameServiceUpdateStub_flat.sol#426-427) is never used and should be removed
ContextUpgradeable._msgData() (EmailNameServiceUpdateStub_flat.sol#432-434) is never used and should be removed
Initializable._disableInitializers() (EmailNameServiceUpdateStub_flat.sol#376-382) is never used and should be removed
Initializable._getInitializedVersion() (EmailNameServiceUpdateStub_flat.sol#387-389) is never used and should be removed
Initializable._isInitializing() (EmailNameServiceUpdateStub_flat.sol#394-396) is never used and should be removed
OwnableUpgradeable.__Ownable_init() (EmailNameServiceUpdateStub_flat.sol#519-521) is never used and should be removed
OwnableUpgradeable.__Ownable_init_unchained() (EmailNameServiceUpdateStub_flat.sol#523-525) is never used and should be removed
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code

Pragma version^0.8.1 (EmailNameServiceUpdateStub_flat.sol#9) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6
Pragma version^0.8.2 (EmailNameServiceUpdateStub_flat.sol#236) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6
Pragma version^0.8.0 (EmailNameServiceUpdateStub_flat.sol#409) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6
Pragma version^0.8.0 (EmailNameServiceUpdateStub_flat.sol#452) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6
Pragma version^0.8.0 (EmailNameServiceUpdateStub_flat.sol#494) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6
Pragma version^0.8.9 (EmailNameServiceUpdateStub_flat.sol#593) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6
solc-0.8.9 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity

Low level call in AddressUpgradeable.sendValue(address,uint256) (EmailNameServiceUpdateStub_flat.sol#65-70):
        - (success) = recipient.call{value: amount}() (EmailNameServiceUpdateStub_flat.sol#68)
Low level call in AddressUpgradeable.functionCallWithValue(address,bytes,uint256,string) (EmailNameServiceUpdateStub_flat.sol#133-142):
        - (success,returndata) = target.call{value: value}(data) (EmailNameServiceUpdateStub_flat.sol#140)
Low level call in AddressUpgradeable.functionStaticCall(address,bytes,string) (EmailNameServiceUpdateStub_flat.sol#160-167):
        - (success,returndata) = target.staticcall(data) (EmailNameServiceUpdateStub_flat.sol#165)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#low-level-calls
```

```
Low level call in AddressUpgradeable.sendValue(address,uint256) (EmailNameServiceUpdateStub_flat.sol#65-70):
        - (success) = recipient.call{value: amount}() (EmailNameServiceUpdateStub_flat.sol#68)
Low level call in AddressUpgradeable.functionCallWithValue(address,bytes,uint256,string) (EmailNameServiceUpdateStub_flat.sol#133-142):
        - (success,returndata) = target.call{value: value}(data) (EmailNameServiceUpdateStub_flat.sol#140)
Low level call in AddressUpgradeable.functionStaticCall(address,bytes,string) (EmailNameServiceUpdateStub_flat.sol#160-167):
        - (success,returndata) = target.staticcall(data) (EmailNameServiceUpdateStub_flat.sol#165)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#low-level-calls

Function ContextUpgradeable.__Context_init() (EmailNameServiceUpdateStub_flat.sol#423-424) is not in mixedCase
Function ContextUpgradeable.__Context_init_unchained() (EmailNameServiceUpdateStub_flat.sol#426-427) is not in mixedCase
Variable ContextUpgradeable.__gap (EmailNameServiceUpdateStub_flat.sol#441) is not in mixedCase
Function OwnableUpgradeable.__Ownable_init() (EmailNameServiceUpdateStub_flat.sol#519-521) is not in mixedCase
Function OwnableUpgradeable.__Ownable_init_unchained() (EmailNameServiceUpdateStub_flat.sol#523-525) is not in mixedCase
Variable OwnableUpgradeable.__gap (EmailNameServiceUpdateStub_flat.sol#584) is not in mixedCase
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions

OwnableUpgradeable.__gap (EmailNameServiceUpdateStub_flat.sol#584) is never used in EmailNameServiceUpdateStub (EmailNameServiceUpdateStub_flat.sol#598-633)
EmailNameServiceUpdateStub.REGISTER_PRICE (EmailNameServiceUpdateStub_flat.sol#618) is never used in EmailNameServiceUpdateStub (EmailNameServiceUpdateStub_flat.sol#598-633)
EmailNameServiceUpdateStub.UPDATE_PRICE (EmailNameServiceUpdateStub_flat.sol#619) is never used in EmailNameServiceUpdateStub (EmailNameServiceUpdateStub_flat.sol#598-633)
EmailNameServiceUpdateStub.donains (EmailNameServiceUpdateStub_flat.sol#623) is never used in EmailNameServiceUpdateStub (EmailNameServiceUpdateStub_flat.sol#598-633)
EmailNameServiceUpdateStub.reverseData (EmailNameServiceUpdateStub_flat.sol#624) is never used in EmailNameServiceUpdateStub (EmailNameServiceUpdateStub_flat.sol#598-633)
EmailNameServiceUpdateStub.priceFeed (EmailNameServiceUpdateStub_flat.sol#626) is never used in EmailNameServiceUpdateStub (EmailNameServiceUpdateStub_flat.sol#598-633)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#unused-state-variable

EmailNameServiceUpdateStub.donainsCount (EmailNameServiceUpdateStub_flat.sol#628) should be constant
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declared-constant

renounceOwnership() should be declared external:
        - OwnableUpgradeable.renounceOwnership() (EmailNameServiceUpdateStub_flat.sol#556-558)
transferOwnership(address) should be declared external:
        - OwnableUpgradeable.transferOwnership(address) (EmailNameServiceUpdateStub_flat.sol#564-567)
helloWorld() should be declared external:
        - EmailNameServiceUpdateStub.helloWorld() (EmailNameServiceUpdateStub_flat.sol#630-632)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#public-function-that-could-be-declared-external
EmailNameServiceUpdateStub_flat.sol analyzed (6 contracts with 75 detectors), 48 result(s) found
ethsec@5188c3820a66:/code/email/contracts$
```

```
Pragma version0.8.9 (BnbUsdQuoteProviderStub.sol#2) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6
solc-0.8.9 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity

Parameter BnbUsdQuoteProviderStub.setPrice(int256)._price (BnbUsdQuoteProviderStub.sol#8) is not in mixedCase
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions

setPrice(int256) should be declared external:
        - BnbUsdQuoteProviderStub.setPrice(int256) (BnbUsdQuoteProviderStub.sol#8-10)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#public-function-that-could-be-declared-external
BnbUsdQuoteProviderStub.sol analyzed (1 contracts with 75 detectors), 4 result(s) found
```

Results

We checked through all of the listed errors and found them to be false positives

Closing Summary

In this report, we have considered the security of the Redefined. We performed our audit according to the procedure described above.

Some issues of Low and informational severity were found, Some suggestions and best practices are also provided in order to improve the code quality and security posture. In The End, Redefined Team resolved all Issues.

Disclaimer

QuillAudits smart contract audit is not a security warranty, investment advice, or an endorsement of the Redefined Platform. This audit does not provide a security or correctness guarantee of the audited smart contracts.

The statements made in this document should not be interpreted as investment or legal advice, nor should its authors be held accountable for decisions made based on them. Securing smart contracts is a multistep process. One audit cannot be considered enough. We recommend that the Redefined Team put in place a bug bounty program to encourage further analysis of the smart contract by other third parties.

About QuillAudits

QuillAudits is a secure smart contracts audit platform designed by QuillHash Technologies. We are a team of dedicated blockchain security experts and smart contract auditors determined to ensure that Smart Contract-based Web3 projects can avail the latest and best security solutions to operate in a trustworthy and risk-free ecosystem.

700+
Audits Completed

$16B
Secured

700K
Lines of Code Audited

Follow Our Journey

Audit Report
March, 2023

For

redefined

QuillAudits

Canada, India, Singapore, United Kingdom

audits.quillhash.com

audits@quillhash.com