StaderLabs - NEARx Staking Reaudit

NEAR Smart Contract Security Audit

Prepared by: **Halborn**

Date of Engagement: **August 29th, 2022 - September 14th, 2022**

Visit: **Halborn.com**

DOCUMENT REVISION HISTORY

VERSION	MODIFICATION	DATE	AUTHOR
0.1	Document Creation	09/01/2022	Thiago Mathias
0.2	Document Update	09/14/2022	Thiago Mathias
0.3	Draft Review	09/15/2022	Timur Guvenkaya
0.4	Draft Review	09/15/2022	Gabi Urrutia
1.0	Remediation Plan	09/16/2022	Thiago Mathias
1.1	Remediation Plan Review	09/16/2022	Timur Guvenkaya
1.2	Remediation Plan Review	09/16/2022	Gabi Urrutia

CONTACTS

CONTACT	COMPANY	EMAIL
Rob Behnke	Halborn	Rob.Behnke@halborn.com
Steven Walbroehl	Halborn	Steven.Walbroehl@halborn.com
Gabi Urrutia	Halborn	Gabi.Urrutia@halborn.com

Timur Guvenkaya	Halborn	Timur.Guvenkaya@halborn.com
Thiago Mathias	Halborn	Thiago.Mathias@halborn.com

EXECUTIVE OVERVIEW

1.1 INTRODUCTION

StaderLabs engaged Halborn to conduct a security audit on their smart contracts beginning on August 29th, 2022 and ending on September 14th, 2022 The security assessment was scoped to the smart contracts provided to the Halborn team.

1.2 AUDIT SUMMARY

The team at Halborn was provided three weeks for the engagement and assigned a full-time security engineer to audit the security of the smart contract. The security engineer is a blockchain and smart-contract security expert with advanced penetration testing, smart-contract hacking, and deep knowledge of multiple blockchain protocols.

The purpose of this audit is to:

- Ensure that smart contract functions operate as intended
- Identify potential security issues with the smart contracts

In summary, Halborn identified an improvement to reduce the likelihood and impact of multiple risks, which has been acknowledged by StaderLabs . The improvement is as follows:

- Replace vulnerable crates.

1.3 TEST APPROACH & METHODOLOGY

RISK METHODOLOGY:

Vulnerabilities or issues observed by Halborn are ranked based on the risk assessment methodology by measuring the **LIKELIHOOD** of a security incident and the **IMPACT** should an incident occur. This framework works for communicating the characteristics and impacts of technology vulnerabilities. The quantitative model ensures repeatable and accurate measurement while enabling users to see the underlying vulnerability characteristics that were used to generate the Risk scores. For every vulnerability, a risk level will be calculated on a scale of 5 to 1 with 5 being the highest likelihood or impact.

RISK SCALE - LIKELIHOOD

5 - Almost certain an incident will occur.
4 - High probability of an incident occurring.
3 - Potential of a security incident in the long term.
2 - Low probability of an incident occurring.
1 - Very unlikely issue will cause an incident.

RISK SCALE - IMPACT

5 - May cause devastating and unrecoverable impact or loss.
4 - May cause a significant level of impact or loss.
3 - May cause a partial impact or loss to many.
2 - May cause temporary impact or loss.
1 - May cause minimal or un-noticeable impact.

The risk level is then calculated using a sum of these two values, creating a value of 10 to 1 with 10 being the highest level of security risk.

CRITICAL	HIGH	MEDIUM	LOW	INFORMATIONAL

10 - CRITICAL
9 - 8 - HIGH
7 - 6 - MEDIUM
5 - 4 - LOW
3 - 1 - VERY LOW AND INFORMATIONAL

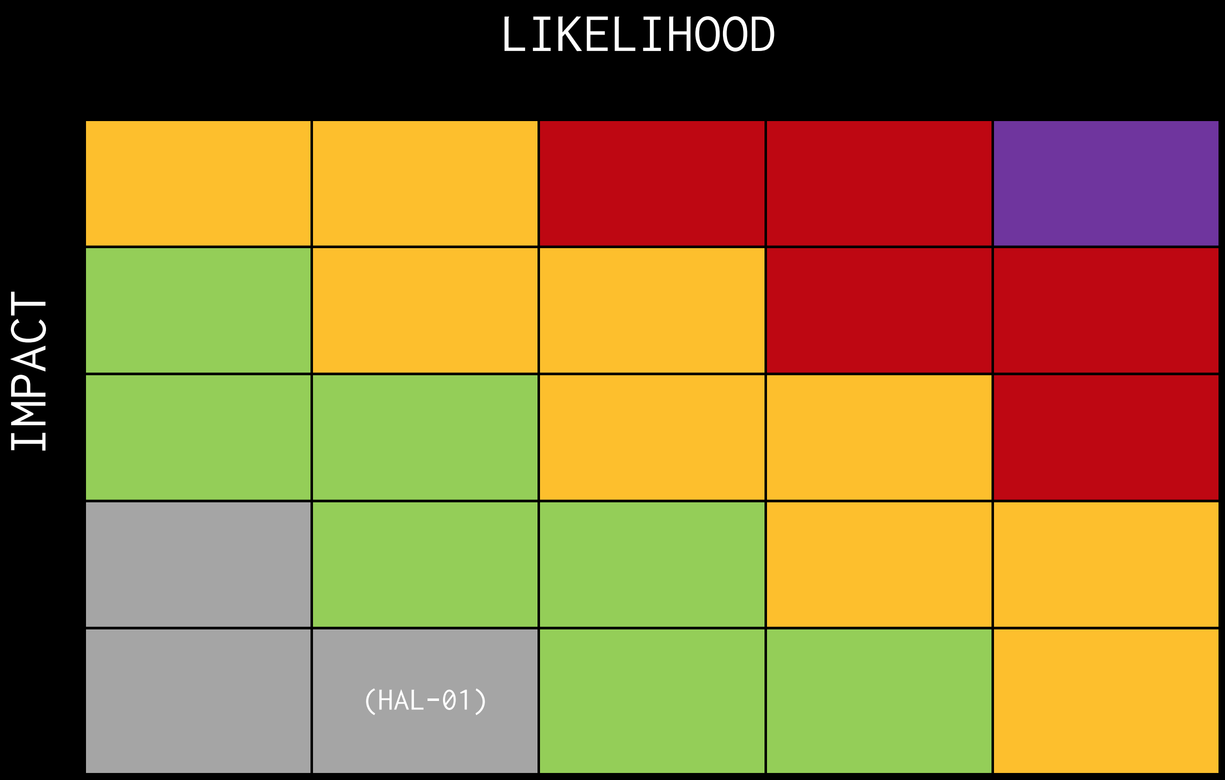
1.4 SCOPE

NEARx contract from **https://github.com/stader-labs/near-liquid-token** commit IDs:

- d75c66f3561530aec068184ae634cdf2cade4cc3
- c667d1ddb7a71a34c6a15d855c14aa1050bac1f1
- edbbdcb04af6de10cd96f5a66c5ed081a6a1151c

2. ASSESSMENT SUMMARY & FINDINGS OVERVIEW

CRITICAL	HIGH	MEDIUM	LOW	INFORMATIONAL
0	0	0	0	1



SECURITY ANALYSIS	RISK LEVEL	REMEDIATION DATE
USAGE OF VULNERABLE CRATES	Informational	ACKNOWLEDGED

FINDINGS & TECH DETAILS

3.1 (HAL-01) USAGE OF VULNERABLE CRATES - INFORMATIONAL

Description:

It was observed that the project uses crates with known vulnerabilities.

Code Location:

ID	package	Short Description
RUSTSEC-2020-0071	time	Potential segfault in the time crate
RUSTSEC-2020-0159	chrono	Potential segfault in localtime_r invocations

Risk Level:

Likelihood - 2
Impact - 1

Recommendation:

Even if those vulnerable crates cannot impact the underlying application, it is advised to be aware of them and attempt to update them to a no-vulnerable version. Furthermore, it is necessary to set up dependency monitoring to always be alerted when a new vulnerability is disclosed in one of the project's crates.
Remediation Plan

ACKNOWLEDGED: The StaderLabs team acknowledged this finding.

THANK YOU FOR CHOOSING

// HALBORN