SPEARBIT

Kiln Security Review

Auditors

Saw-mon and Natalie, Lead Security Researcher

Report prepared by: Pablo Misirov

September 22, 2023

Contents

1 About Spearbit 2

2 Introduction 2

3 Risk classification 2
3.1 Impact 2
3.2 Likelihood 2
3.3 Action required for severity levels 2

4 Executive Summary 3

5 Findings 4
5.1 Gas Optimization 4
5.1.1 Length checks for the endpoint inputs can be optimised 4
5.2 Informational 4
5.2.1 NatSpec comment missing for `amountPerValidator` 4
5.2.2 Formatting and typos 5
5.2.3 `msg.value` verification is missing from the non-custom endpoints 5

1 About Spearbit

Spearbit is a decentralized network of expert security engineers offering reviews and other security related services to Web3 projects with the goal of creating a stronger ecosystem. Our network has experience on every part of the blockchain technology stack, including but not limited to protocol design, smart contracts and the Solidity compiler. Spearbit brings in untapped security talent by enabling expert freelance auditors seeking flexibility to work on interesting projects together.

Learn more about us at spearbit.com

2 Introduction

Vyper contract for batched deposits to the Ethereum beacon chain deposit contract

Disclaimer: This security review does not guarantee against a hack. It is a snapshot in time of vyper-batch-deposit according to the specific commit. Any modifications to the code will require a new security review.

3 Risk classification

Severity level	**Impact: High**	**Impact: Medium**	**Impact: Low**
Likelihood: high	Critical	High	Medium
Likelihood: medium	High	Medium	Low
Likelihood: low	Medium	Low	Low

3.1 Impact

- High - leads to a loss of a significant portion (>10%) of assets in the protocol, or significant harm to a majority of users.
- Medium - global losses <10% or losses to only a subset of users, but still unacceptable.
- Low - losses will be annoying but bearable--applies to things like griefing attacks that can be easily repaired or even gas inefficiencies.

3.2 Likelihood

- High - almost certain to happen, easy to perform, or not easy but highly incentivized
- Medium - only conditionally possible or incentivized, but still relatively likely
- Low - requires stars to align, or little-to-no incentive

3.3 Action required for severity levels

- Critical - Must fix as soon as possible (if already deployed)
- High - Must fix (before deployment if not already deployed)
- Medium - Should fix
- Low - Could fix

4 Executive Summary

Over the course of 1 days in total, Kiln engaged with Spearbit to review the vyper-batch-deposit protocol. In this period of time a total of **4** issues were found.

Summary

Project Name	Kiln
Repository	vyper-batch-deposit
Commit	64cf2b...09e9
Type of Project	Batch Deposit, ETH2
Audit Timeline	Sep 5 - Sep 6
Fix period	Sep 6 - Sep 11

Issues Found

Severity	**Count**	**Fixed**	**Acknowledged**
Critical Risk	0	0	0
High Risk	0	0	0
Medium Risk	0	0	0
Low Risk	0	0	0
Gas Optimizations	1	1	0
Informational	3	3	0
Total	**4**	**4**	**0**

5 Findings

5.1 Gas Optimization

5.1.1 Length checks for the endpoint inputs can be optimised

Severity: Gas Optimization

Context:

- BatchDeposit.vy#L44-L50
- BatchDeposit.vy#L84-L91
- BatchDeposit.vy#L124-L130
- BatchDeposit.vy#L164-L171

Description: In all the `4` endpoints we perform the following length checks:

In other words we check `len(x) % X == 0` and `l = len(x) / X`. One can combine these two checks into one:

also by not declaring `l` we would say on `mstore` and `mload`.

Recommendation: The code in this context can be changed to

and for the two endpoints with `amountPerValidator` and extra edit:

```
- if amountPerValidator * l != msg.value:
+ if amountPerValidator * len(dataRoots) != msg.value:
```

Kiln: Fixed in `05832bba18ad54652bd66145a22c4027c903a14c`.

Spearbit: Fixed.

5.2 Informational

5.2.1 NatSpec comment missing for `amountPerValidator`

Severity: Informational

Context:

- BatchDeposit.vy#L74
- BatchDeposit.vy#L154

Description: NatSpec comment `@param amountPerValidator` is missing in this context.

Recommendation: Comments should be added for `amountPerValidator`.

Kiln: Fixed in `9f4b85f998050d7f2b66bb5e029023dc6f9c1c0e`.

Spearbit: Fixed.

5.2.2 Formatting and typos

Severity: Informational

Context:

- BatchDeposit.vy#L39
- BatchDeposit.vy#L79
- BatchDeposit.vy#L119
- BatchDeposit.vy#L159

Description:

- Code formatting (indentation) is not consistent across all `4` endpoints.
- In the above context there is a typo in the NatSpec comment: `pulbicKeys` (should be `publicKeys`)

Recommendation: Formatting and typos can be corrected.

Kiln: Fixed in `27627135c961b54209e390aff3f39362b2b68a10`.

Spearbit: Fixed.

5.2.3 `msg.value` verification is missing from the non-custom endpoints

Severity: Informational

Context:

- BatchDeposit.vy#L32
- BatchDeposit.vy#L112

Description: The custom endpoints `batchDepositCustom` and `bigBatchDepositCustom` have the following verification check for the `msg.value` provided:

The corresponding checkpoint is missing for `batchDeposit` and `bigBatchDeposit`.

Recommendation: For consistency it might be best to add the relevant check for the non-custom endpoints. Note that it would increase the gas cost for when enough native tokens are provided. But in the case of failure it would actually save gas.

Kiln: Fixed in `c3000b83a87bc2cbd4257090d1a9d8150d9d21d4`.

Spearbit: Fixed.