METATRUST

Security Assessment for

Pell Network

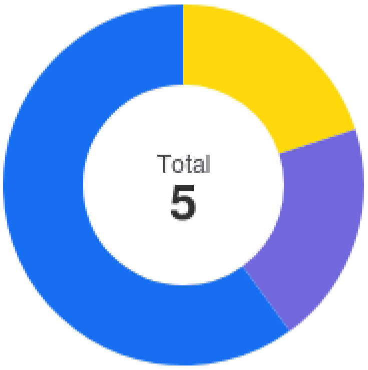
April 28, 2024

Executive Summary

Overview	
Project Name	Pell Network
Codebase URL	https://github.com/0xPellNetwork/restaking-contracts
Scan Engine	Security Analyzer
Scan Time	2024/04/28 08:00:00
Commit Id	0ab105fa0811b8486af0ecf84a263db42dc1edff 8add8b89019f27f83fc5f29d4ea32f13bd032770

Critical Issues	The issue can cause large economic losses, large-scale data disorder, loss of control of authority management, failure of key functions, or indirectly affect the correct operation of other smart contracts interacting with it.
High Risk Issues	The issue puts a large number of users' sensitive information at risk or is reasonably likely to lead to catastrophic impacts on clients' reputations or serious financial implications for clients and users.
Medium Risk Issues	The issue puts a subset of users' sensitive information at risk, would be detrimental to the client's reputation if exploited, or is reasonably likely to lead to moderate financial impact.
Low Risk Issues	The risk is relatively small and could not be exploited on a recurring basis, or is a risk that the client has indicated is low-impact in view of the client's business circumstances.
Informational Issue	The issue does not pose an immediate risk but is relevant to security best practices or Defence in Depth.

Total	
Critical Issues	0
High risk Issues	0
Medium risk Issues	1
Low risk Issues	1
Informational Issues	3



Critical Issues	0%	**0**
High risk Issues	0%	**0**
Medium risk Issues	20%	**1**
Low risk Issues	20%	**1**
Informational Issues	60%	**3**

Summary of Findings

MetaScan security assessment was performed on **April 28, 2024 08:00:00** on project **Pell Network** with the repository on branch **default branch**. The assessment was carried out by scanning the project's codebase using the scan engine **Security Analyzer**. There are in total **5** vulnerabilities / security risks discovered during the scanning session, among which **1** medium risk vulnerabilities, **1** low risk vulnerabilities, **3** informational issues.

ID	Description	Severity	Alleviation
MSA-001	Centralization Risk	Medium risk	Acknowledged
MSA-002	A two-step process for transferring the ownership is recommended	Low risk	Acknowledged
MSA-003	Redundant state variable	Informational	Fixed
MSA-004	The size of gap	Informational	Acknowledged
MSA-005	Misleading comments	Informational	Fixed

Findings

Medium risk (1)

1. Centralization Risk

Medium risk Security Analyzer

In the `DelegationManager` contract, the owner has the privilege of the following functions:

- `setMinWithdrawalDelay`: Owner-only function for modifying the value of the `minWithdrawalDelay` variable.
- `setStrategyWithdrawalDelay`: Called by owner to set the minimum withdrawal delay for each passed in strategy.

In the `StrategyManager` contract, the owner has the privilege of the following functions:

- `setStrategyWhitelister`: Owner-only function to change the `strategyWhitelister` address.

File(s) Affected

restaking-contracts-audit/contracts/core/DelegationManager.sol #350-363

```
function setMinWithdrawalDelay(uint256 newMinWithdrawalDelay) external onlyOwner {
  _setMinWithdrawalDelay(newMinWithdrawalDelay);
}

/**
 * @notice Called by owner to set the minimum withdrawal delay for each passed in strategy
 * Note that the min cooldown to complete a withdrawal of a strategy is
 * MAX(minWithdrawalDelay, strategyWithdrawalDelay[strategy])
 * @param strategies The strategies to set the minimum withdrawal delay for
 * @param withdrawalDelay The minimum withdrawal delay to set for each strategy
 */
function setStrategyWithdrawalDelay(IStrategy[] calldata strategies, uint256[] calldata withdrawalDel
  _setStrategyWithdrawalDelay(strategies, withdrawalDelay);
}
```

restaking-contracts-audit/contracts/core/StrategyManager.sol #117-119

```
  IERC20 token,
  uint256 amount,
  address staker,
```

Recommendation

Consider implementing a decentralized governance mechanism or a multi-signature scheme that requires consensus among multiple parties before pausing or unpausing the contract. This can help mitigate the centralization risk associated with a single owner controlling critical contract functions. Alternatively, you can provide a clear justification for the centralization aspect and ensure that users are aware of the potential risks associated with a single point of control.

Alleviation Acknowledged

The team acknowledged this finding.

Low risk (1)

1. A two-step process for transferring the ownership is recommended

Low risk

Security Analyzer

In contract `DelegationManager`, and `OwnableUpgradeable`, it is possible that the owner role transfers ownership to the wrong address by mistake, resulting in authorization loss from the team. So, a two-step process for transferring the ownership is recommended

Reference: Ownable2StepUpgradeable

File(s) Affected

restaking-contracts-audit/contracts/core/DelegationManager.sol #19-19

```
19  contract DelegationManager is Initializable, OwnableUpgradeable, Pausable, DelegationManagerStorage, Ree
```

restaking-contracts-audit/contracts/core/StrategyManager.sol #20-20

```
20  contract StrategyManager is Initializable, OwnableUpgradeable, ReentrancyGuardUpgradeable, Pausable, Str
```

Recommendation

Consider using the Ownable2StepUpgradeable contract and calling its `_transferOwnership` for a two-step ownership transfer.

Alleviation Acknowledged

The team acknowledged this finding.

Informational (3)

1. Redundant state variable

Informational

Security Analyzer

The state variable `beaconChainETHSharesToDecrementOnWithdrawal` turns useless after the related contracts removed. So it is can be removed.

File(s) Affected

restaking-contracts-audit/contracts/core/StrategyManagerStorage.sol #56-61

```
56    /*
57     * Reserved space previously used by the deprecated mapping(address => uint256) beaconChainETHSharesTo
58     * This mapping tracked beaconChainETH "deficit" in cases where updates were made to shares retroactiv
59     * moved into the EigenPodManager contract itself.
60     */
61    mapping(address => uint256) internal beaconChainETHSharesToDecrementOnWithdrawal;
```

Recommendation

Removing redundant state variable.

Alleviation Fixed

The team addressed this finding by removing the redundant state variable in the commit 75fcd906f98292f446823ea59bb2fa5b1eb61606.

2. The size of gap

Informational

Security Analyzer

Due to one state variable is removed from the contract, the size of the gap need to be increased by one, to 40, rather than 49, from 39.

File(s) Affected

restaking-contracts-audit/contracts/core/StrategyManagerStorage.sol #80-80

```
80    uint256[49] private __gap;
```

Recommendation

Updating the size of the gap.

Alleviation Acknowledged

The team acknowledged this finding.

3. Misleading comments

Informational   Security Analyzer

The comments in the `DelegationManager` contract describes logic related to the `EigenPodManagerContract`, `EigenPodManager`, and `EigenPod`, which do not exist in the protocol.

File(s) Affected

restaking-contracts-audit/contracts/core/DelegationManager.sol #606-606

```
606     * `staker`s EigenPod; otherwise a call is ultimately forwarded to the `strategy` with info on the `t
```

restaking-contracts-audit/contracts/core/DelegationManager.sol #315-315

```
315     * @dev Callable only by the StrategyManager or EigenPodManager.
```

restaking-contracts-audit/contracts/core/DelegationManager.sol #35-35

```
35    // @notice Simple permission for functions that are only callable by the StrategyManager contract OR b
```

Recommendation

Recommend removing misleading comments.

Alleviation Fixed

The team addressed this finding by removing misleading comments, in the commit 8add8b89019f27f83fc5f29d4ea32f13bd032770.

Audit Scope

File	SHA256	File Path
PauserRegistry.sol	f9fb892072f27acd75740d9be49095a099736b46fa002e276025b3a593606382	/contracts/permissions/PauserRegistry.sol
Pausable.sol	c15bc3c1164974771f98289c05f028f4bc21a3573f78d0e8eaf231cf3211c45b	/contracts/permissions/Pausable.sol
UpgradeableSignatureCheckingUtils.sol	d792392f38eb56c6284df75c63499636b91a3b1aecf6909f3abae85a38c031eb	/contracts/utils/UpgradeableSignatureCheckingUtils.sol
DelegationManager.sol	82601fadabdc0f99cc2411840500b970398eceb4412b61b40d4661849bdb0eb0	/contracts/core/DelegationManager.sol
StrategyManagerStorage.sol	b977cdd2c8e23699c8294d20f43ab850f2c8bee790ea090879dfbfadbe7ac292	/contracts/core/StrategyManagerStorage.sol
Slasher.sol	6dbf0682b9e0d135512cbf4a0dea8b65fbdd1023e1cc13000fee120cd7fbdb64	/contracts/core/Slasher.sol
StrategyManager.sol	a4d9cfee3dd182ccd2bee20beb6a6e4ec9d40c7dc7a95db3b790e5ffe60c6d43	/contracts/core/StrategyManager.sol
DelegationManagerStorage.sol	27b5ad29b55b025af8e540f339a852fc8f67163f7e8b3db17c01598dcc2bb937	/contracts/core/DelegationManagerStorage.sol
StrategyBaseTVLLimits.sol	084aa9f1de3993d8783621e3e74328d9cc89797bbc3056fd72e76113352bea9f	/contracts/strategies/StrategyBaseTVLLimits.sol
StrategyBase.sol	36042cfeec871276fa570937a5afbdc33d328fff1e192ad80f8f9cb78dcf9b9b	/contracts/strategies/StrategyBase.sol
Endian.sol	979c07e66b99ca52572f6a545235eded0143126dad75430e96490ec1973de18d	/contracts/libraries/Endian.sol
Merkle.sol	c150ab5e94ad975e42d10f6edc05431a5e093653d3f0c00326ef4ac601149e72	/contracts/libraries/Merkle.sol
StructuredLinkedList.sol	c376766b5562639e9fa40daa0a4cd1a3d93ae6286284c17be1ca444fcaa4430f	/contracts/libraries/StructuredLinkedList.sol
EIP1271SignatureUtils.sol	14618b104bc246bca1febb2d0424e0e0aa954e586d711035ba7367e99ebc15c5	/contracts/libraries/EIP1271SignatureUtils.sol
BytesLib.sol	f7959684dab3cf2753b456806dab33e22dde53bf8bb9314dd4df70d28feb6b9b	/contracts/libraries/BytesLib.sol

Disclaimer

This report is governed by the stipulations (including but not limited to service descriptions, confidentiality, disclaimers, and liability limitations) outlined in the Services Agreement, or as detailed in the scope of services and terms provided to you, the Customer or Company, within the context of the Agreement. The Company is permitted to use this report only as allowed under the terms of the Agreement. Without explicit written permission from MetaTrust, this report must not be shared, disclosed, referenced, or depended upon by any third parties, nor should copies be distributed to anyone other than the Company.

It is important to clarify that this report neither endorses nor disapproves any specific project or team. It should not be viewed as a reflection of the economic value or potential of any product or asset developed by teams or projects engaging MetaTrust for security evaluations. This report does not guarantee that the technology assessed is completely free of bugs, nor does it comment on the business practices, models, or legal compliance of the technology's creators.

This report is not intended to serve as investment advice or a tool for investment decisions related to any project. It represents a thorough assessment process aimed at enhancing code quality and mitigating risks inherent in cryptographic tokens and blockchain technology. Blockchain and cryptographic assets inherently carry ongoing risks. MetaTrust's role is to support companies and individuals in their security diligence and to reduce risks associated with the use of emerging and evolving technologies. However, MetaTrust does not guarantee the security or functionality of the technologies it evaluates.

MetaTrust's assessment services are contingent on various dependencies and are continuously evolving. Accessing or using these services, including reports and materials, is at your own risk, on an as-is and as-available basis. Cryptographic tokens are novel technologies with inherent technical risks and uncertainties. The assessment reports may contain inaccuracies, such as false positives or negatives, and unpredictable outcomes. The services may rely on multiple third-party layers.

All services, labels, assessment reports, work products, and other materials, or any results from their use, are provided "as is" and "as available," with all faults and defects, without any warranty. MetaTrust expressly disclaims all warranties, whether express, implied, statutory, or otherwise, including but not limited to warranties of merchantability, fitness for a particular purpose, title, non-infringement, and any warranties arising from course of dealing, usage, or trade practice. MetaTrust does not guarantee that the services, reports, or materials will meet specific requirements, be error-free, or be compatible with other software, systems, or services.

Neither MetaTrust nor its agents make any representations or warranties regarding the accuracy, reliability, or currency of any content provided through the services. MetaTrust is not liable for any content inaccuracies, personal injuries, property damages, or any loss resulting from the use of the services, reports, or materials.

Third-party materials are provided "as is," and any warranty concerning them is strictly between the Customer and the third-party owner or distributor. The services, reports, and materials are intended solely for the Customer and should not be relied upon by others or shared without MetaTrust's consent. No third party or representative thereof shall have any rights or claims against MetaTrust regarding these services, reports, or materials.

The provisions and warranties of MetaTrust in this agreement are exclusively for the Customer's benefit. No third party has any rights or claims against MetaTrust regarding these provisions or warranties. For clarity, the services, including any assessment reports or materials, should not be used as financial, tax, legal, regulatory, or other forms of advice.