METATRUST

Security Assessment for

NodeDAO

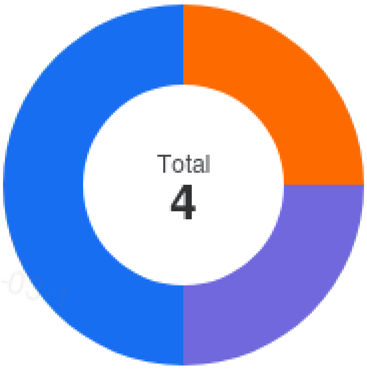
March 1, 2023

Executive Summary

Overview	
Project Name	NodeDAO
Codebase Path	git://github.com/node_dao
Scan Engine	Security Analyzer
Scan Time	2023/03/1 15:28:26
Source Code	node_dao commit:-

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	1
Medium risk Issues	0
Low risk Issues	1
Informational Issues	2



Critical Issues	0%	**0**
High risk Issues	25%	**1**
Medium risk Issues	0%	**0**
Low risk Issues	25%	**1**
Informational Issues	50%	**2**

Summary of Findings

MetaScan security assessment was performed on **March 1, 2023 15:28:26** on project **NodeDAO** with the repository **node_dao** 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 **4** vulnerabilities / security risks discovered during the scanning session, among which **0** critical vulnerabilities, **1** high risk vulnerabilities, **0** medium risk vulnerabilities, **1** low risk vulnerabilities, **2** informational issues.

ID	Description	Severity	Alleviation
MSA-001	Overflow of Bit Shift Operation	High risk	Fixed
MSA-002	Lack of check in assignBlacklistOrQuitOperator	Low risk	Acknowledged
MSA-003	Lack of Check the isQuit Status	Informational	Fixed
MSA-004	Overflow of Bit Shift Operation	Informational	Acknowledged

Findings

Critical (0)

No Critical vulnerabilities found here

High risk (1)

1. Overflow of Bit Shift Operation High risk Security Analyzer

There are bit shift operations in the BeaconOracle contract to mark the statuses of the members: uint256 bitMask = reportBitMaskPosition; uint256 mask = 1 << index; require(bitMask & mask == 0, "ALREADY_SUBMITTED"); However, there is no limitation on the index to keep the bit shift operation safe. For example, the calculation of i << index will always be zero if the index is greater than 255. and Poc is following: The following steps are performed to prove that once the number of Oracle members is greater than 255, an unexpected result will happen.

- Add an Oracle member address(11)
- Check whether the address(11) member is a reported beacon, the result is false;
- Impersonate the member address(11) and call the reportBeacon() function;
- Check whether the address(11) member is a reported beacon, the result turns true;
- Add 255 Oracle members;
- add the Oracle member address(1255)
- Check whether the address(1255) member is a reported beacon, the result is false;
- Impersonate the member address(1255) and call the reportBeacon() function;
- Check whether the address(1255) member is a reported beacon, the result turns false instead of true;

File(s) Affected

src/oracle/BeaconOracle.sol #169-190 #341-349 #140-148

Examples

Recommendation

We advise adding a range check on the number of Oracle members to prevent the overflow of the bit shift operation.

Alleviation Fixed

-

Medium risk (0)

No Medium risk vulnerabilities found here

Low risk (1)

1. Lack of check in assignBlacklistOrQuitOperator

Low risk Security Analyzer

When distributing funds to other operators, the function allows the owner to assign the funds of a blacklist operator to a quit operator. Since there is no check on whether the assignOperatorId has quit, it is possible to assign funds to a quit operator, which may result in the funds being wasted.

File(s) Affected

src/LiquidStaking.sol #130-156

Examples

```

        // Update operator available funds
        uint256 totalAmount = 0;
        for (uint256 i = 0; i < _operatorIds.length; ++i) {
            uint256 operatorId = _operatorIds[i];
            require(nodeOperatorRegistryContract.isTrustedOperator(operatorId), "Operator must be trust
            uint256 amount = _amounts[i];
            totalAmount += amount;
            operatorPoolBalances[operatorId] += amount;
        }

        require(operatorPoolBalances[_assignOperatorId] >= totalAmount, "Insufficient balance of blackl
        operatorPoolBalances[_assignOperatorId] -= totalAmount;
```

Recommendation

Add check of the operator if quit

Alleviation Acknowledged

The exit situation has been filtered in the isTrustedOperator method

Informational (2)

1. Lack of Check the isQuit Status

Informational Security Analyzer

The operator's owner can quit many times by calling the quitOperator() function. To prevent any potential side effects in the future, validating the status of isQuit is good practice.

File(s) Affected

src/registries/NodeOperatorRegistry.sol #220-237

Examples

```
    function quitOperator(uint256 _operatorId, address _to) external {
        NodeOperator memory operator = operators[_operatorId];
        require(operator.owner == msg.sender, "PERMISSION_DENIED");
  •••
        emit OperatorQuit(_operatorId, nowPledge, _to);
    }

```

Recommendation

We advise checking the status of the isQuit in the quitOperator function.

Alleviation Fixed

The number of nft operators that can be exited must be 0. Operators that have exited can only execute this nft

2. Overflow of Bit Shift Operation

Informational Security Analyzer

In the LiquidityStaking contract

- the centralized role owner has permission for the following functions:
  - assignBlacklistOrQuitOperator: update the operatorPoolBalances for the specified operator.
  - slashOperator: update the operatorPoolBalances for the specified operatorId
  - setDaoAddress: update the dao
- the centralized role dao has permission for the following functions:
  - setDaoVaultAddress: update the daoVaultAddress
  - setDepositFeeRate: update the depositFeeRate
  - setLiquidStakingWithdrawalCredentials: update the liquidStakingWithdrawalCredentials
  - setBeaconOracleContract: update the beaconOracleContract
  - setNodeOperatorRegistryContract: update the nodeOperatorRegistryContract
  - pause: pause the contract
  - unpause: unpause the contract In the ConsensusVault contract
- the centralized role owner and dao has permission for the following functions:
  - setDaoAddress: update the dao address
  - setLiquidStaking: update the liquidStakingContractAddress
  - transfer: transfer funds from the contract to a specified address In the ELVault contract
- the centralized role dao has permission for the following functions:
  - setLiquidStaking: update the liquidStakingContract
  - setPublicSettleLimit: update the publicSettleLimit;
  - setComissionRate: update the comissionRate;
  - setDaoComissionRate: update the daoComissionRate;
  - setDaoAddress:update the dao.
- the centralized role liquidStakingContract has permission for the following functions:
  - settle: Settles outstanding rewards
  - reinvestmentOfLiquidStaking: update the unclaimedRewards
  - claimRewardsOfUser: Claims the rewards belonging to a validator nft and transfer it to the owner
  - setUserNft: update the uerNftCounts and userGasHeight for the specified _tokenId
  - setLiquidStakingGasHeight: update the liquidStakingGasHeight
- the centralized role nodeOperatorRegistryContract has permission for the following functions:
  - claimOperatorRewards: update the operatorRewards and distribute rewards to the specified addresses, while updating the collateral balance based on the number of NFTs held.
  - claimDaoRewards: update the daoRewards, setting it to 0, and transferring the rewards obtained to the specified address In the ELVaultFactory contract:
- The centralized role owner has permission for the following function:
  - setNodeOperatorRegistry: update the nodeOperatorRegistryAddress
  - setDaoAddress: update the dao In the VNFT contract:
- the centralized role liquidstaking has permission for the following function:
  - whiteListMint: Mints a Validator nft (vNFT)
  - whiteListBurn: update the lastOwners, operatorRecords. Burns a Validator nft (vNFT)
- The centralized role owner has permission for the following function
  - setBaseURI:update the _baseTokenURI
  - setLiquidStaking:update the liquidStakingContractAddress In the BeaconOracle contract
- The centralized role Dao has permission for the following function
  - setDaoAddress: update the dao;
  - addOracleMember: update the oracleMembers;
  - removeOracleMember: update the oracleMembers;
  - resetEpochsPerFrame:update the epochsPerFrame;
  - setLiquidStaking:update the liquidStakingContractAddress.
- The centralized role liquidStaking has permission for the following function
  - addPendingBalances: update the pendingBalances; In the NodeOperatorRegistry contract:
- The centralized role Dao has permission for the following function:

- setTrustedOperator: update the operators.trusted for the specified _id, update the totalTrustedOperators, and update the trustedControllerAddress for the specified operator.controllerAddress
- removeTrustedOperator: delete the operators.trusted for the specified _id, update the totalTrustedOperators, and update the trustedControllerAddress for the specified operator.controllerAddress
- setBlacklistOperator: update the blacklistOperators for the specified _id, update the totalBlacklistOperators
- removeBlacklistOperator: update the blacklistOperators for the specified _id, update the totalBlacklistOperators

File(s) Affected

src/oracle/BeaconOracle.sol #1-424
src/registries/NodeOperatorRegistry.sol #1-656
src/tokens/VNFT.sol #1-364
src/vault/ConsensusVault.sol #1-84
src/vault/ELVault.sol #1-394
src/vault/ELVaultFactory.sol #1-90
src/LiquidStaking.sol #1-584

Examples

Recommendation

We advise using the multi-signature wallet and the timelock to mitigate the centralized role issue.

Alleviation Acknowledged

OnlyOwner adopts time-lock+multi-signature OnlyDao takes multiple signatures

Disclaimer

This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, disclaimer and limitation of liability) set forth in the Services Agreement, or the scope of services, and terms and conditions provided to you ("Customer" or the "Company") in connection with the Agreement. This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes, nor may copies be delivered to any other person other than the Company, without MetaTrust's prior written consent in each instance.

This report is not, nor should be considered, an "endorsement" or "disapproval" of any particular project or team. This report is not, nor should be considered, an indication of the economics or value of any "product" or "asset" created by any team or project that contracts MetaTrust to perform a security assessment. This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors, business, business model or legal compliance.

This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk. MetaTrust's position is that each company and individual are responsible for their own due diligence and continuous security. MetaTrust's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies, and in no way claims any guarantee of security or functionality of the technology we agree to analyze.

The assessment services provided by MetaTrust is subject to dependencies and under continuing development. You agree that your access and/or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives, and other unpredictable results. The services may access, and depend upon, multiple layers of third-parties.

ALL SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF ARE PROVIDED "AS IS" AND "AS Security Assessment AVAILABLE" AND WITH ALL FAULTS AND DEFECTS WITHOUT WARRANTY OF ANY KIND. TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, MetaTrust HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS. WITHOUT LIMITING THE FOREGOING, MetaTrust SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM COURSE OF DEALING, USAGE, OR TRADE PRACTICE. WITHOUT LIMITING THE FOREGOING, MetaTrust MAKES NO WARRANTY OF ANY KIND THAT THE SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF, WILL MEET CUSTOMER'S OR ANY OTHER PERSON'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULT, BE COMPATIBLE OR WORK WITH ANY SOFTWARE, SYSTEM, OR OTHER SERVICES, OR BE SECURE, ACCURATE, COMPLETE, FREE OF HARMFUL CODE, OR ERROR-FREE. WITHOUT LIMITATION TO THE FOREGOING, MetaTrust PROVIDES NO WARRANTY OR UNDERTAKING, AND MAKES NO REPRESENTATION OF ANY KIND THAT THE SERVICE WILL MEET CUSTOMER'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULTS, BE COMPATIBLE OR WORK WITH ANY OTHER SOFTWARE, APPLICATIONS, SYSTEMS OR SERVICES, OPERATE WITHOUT INTERRUPTION, MEET ANY PERFORMANCE OR RELIABILITY STANDARDS OR BE ERROR FREE OR THAT ANY ERRORS OR DEFECTS CAN OR WILL BE CORRECTED.

WITHOUT LIMITING THE FOREGOING, NEITHER MetaTrust NOR ANY OF MetaTrust'S AGENTS MAKES ANY REPRESENTATION OR WARRANTY OF ANY KIND, EXPRESS OR IMPLIED AS TO THE ACCURACY, RELIABILITY, OR CURRENCY OF ANY INFORMATION OR CONTENT PROVIDED THROUGH THE SERVICE. MetaTrust WILL ASSUME NO LIABILITY OR RESPONSIBILITY FOR (I) ANY ERRORS, MISTAKES, OR INACCURACIES OF CONTENT AND MATERIALS OR FOR ANY LOSS OR DAMAGE OF ANY KIND INCURRED AS A RESULT OF THE USE OF ANY CONTENT, OR (II) ANY PERSONAL INJURY OR PROPERTY DAMAGE, OF ANY NATURE WHATSOEVER, RESULTING FROM CUSTOMER'S ACCESS TO OR USE OF THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS.

ALL THIRD-PARTY MATERIALS ARE PROVIDED "AS IS" AND ANY REPRESENTATION OR WARRANTY OF OR CONCERNING ANY THIRD-PARTY MATERIALS IS STRICTLY BETWEEN CUSTOMER AND THE THIRD-PARTY OWNER OR DISTRIBUTOR OF THE THIRD-PARTY MATERIALS.

THE SERVICES, ASSESSMENT REPORT, AND ANY OTHER MATERIALS HEREUNDER ARE SOLELY PROVIDED TO CUSTOMER AND MAY NOT BE RELIED ON BY ANY OTHER PERSON OR FOR ANY PURPOSE NOT SPECIFICALLY IDENTIFIED IN THIS AGREEMENT, NOR MAY COPIES BE DELIVERED TO, ANY OTHER PERSON WITHOUT MetaTrust'S PRIOR WRITTEN CONSENT IN EACH INSTANCE.

NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING Security Assessment MATERIALS AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST MetaTrust WITH RESPECT TO SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING MATERIALS.

THE REPRESENTATIONS AND WARRANTIES OF MetaTrust CONTAINED IN THIS AGREEMENT ARE SOLELY FOR THE BENEFIT OF CUSTOMER. ACCORDINGLY, NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH REPRESENTATIONS AND WARRANTIES AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST MetaTrust WITH RESPECT TO SUCH REPRESENTATIONS OR WARRANTIES OR ANY MATTER SUBJECT TO OR RESULTING IN INDEMNIFICATION UNDER THIS AGREEMENT OR OTHERWISE.

FOR AVOIDANCE OF DOUBT, THE SERVICES, INCLUDING ANY ASSOCIATED ASSESSMENT REPORTS OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.