Kommunitas

Smart Contract Security Audit

Prepared by ShellBoxes

December 1, 2021 - January 11, 2022

Shellboxes.com

contact@shellboxes.com

Document Properties

Client	Kommunitas
Version	1.0
Classification	Public

Scope

The Kommunitas Contract in the Kommunitas Repository

Repo	Commit Hash
https://github.com/Kommunitas-net/Launchpad_Core	058a3ee5bd86180062495b3e71c2f3ce84d0baa9

Files	MD5 Hash
KommunitasFactory.sol	675794678632e0811070f55170cf8d49
KommunitasProject.sol	fc832bf6894f2e464e0abd98d0bf282d

Re-Audit

Repo	Commit Hash
https://github.com/Kommunitas-net/Launchpad_Core	932e775da5b620f1ee9b3a34a026180db71f8fc0

Contacts

COMPANY	EMAIL
ShellBoxes	contact@shellboxes.com

Contents

1 Introduction

Kommunitas engaged ShellBoxes to conduct a security assessment on the Kommunitas beginning on December 1, 2021 and ending January 11, 2022. In this report, we detail our methodical approach to evaluate potential security issues associated with the implementation of smart contracts, by exposing possible semantic discrepancies between the smart contract code and design document, and by recommending additional ideas to optimize the existing code. Our findings indicate that the current version of smart contracts can still be enhanced further due to the presence of many security and performance concerns.

This document summarizes the findings of our audit.

1.1 About Kommunitas

Kommunitas is a decentralized and tier-less Launchpad. Kommunitas is the solution for Multi Chain oriented projects. Kommunitas welcomes project from various blockchain like Polygon, BSC, Ethereum, Avalance, Solana, etc...

Issuer	Kommunitas
Website	`https://kommunitas.net/`
Type	Solidity Smart Contract
Audit Method	Whitebox

1.2 Approach & Methodology

ShellBoxes used a combination of manual and automated security testing to achieve a balance between efficiency, timeliness, practicability, and correctness within the audit's scope. While manual testing is advised for identifying problems in logic, procedure, and implementation, automated testing techniques help to expand the coverage of smart contracts and can quickly detect code that does not comply with security best practices.

1.2.1 Risk Methodology

Vulnerabilities or bugs identified by ShellBoxes are ranked using a risk assessment technique that considers both the LIKELIHOOD and IMPACT of a security incident. This framework is effective at conveying the features and consequences of technological vulnerabilities.

Its quantitative paradigm enables repeatable and precise measurement, while also revealing the underlying susceptibility characteristics that were used to calculate the Risk scores. A risk level will be assigned to each vulnerability on a scale of 5 to 1, with 5 indicating the greatest possibility or impact.

- Likelihood quantifies the probability of a certain vulnerability being discovered and exploited in the untamed.
- Impact quantifies the technical and economic costs of a successful attack.
- Severity indicates the risk's overall criticality.

Probability and impact are classified into three categories: H, M, and L, which correspond to high, medium, and low, respectively. Severity is determined by probability and impact and is categorized into four levels, namely Critical, High, Medium, and Low.

Impact	Likelihood: High	Likelihood: Medium	Likelihood: Low
High	Critical	High	Medium
Medium	High	Medium	Low
Low	Medium	Low	Low

2 Findings Overview

2.1 Summary

The following is a synopsis of our conclusions from our analysis of the Kommunitas implementation. During the first part of our audit, we examine the smart contract source code and run the codebase via a static code analyzer. The objective here is to find known coding problems statically and then manually check (reject or confirm) issues highlighted by the tool. Additionally, we check business logics, system processes, and DeFi-related components manually to identify potential hazards and/or defects.

2.2 Key Findings

In general, these smart contracts are well-designed and constructed, but their implementation might be improved by addressing the discovered flaws, which include , 1 high-severity, 2 medium-severity, 4 low-severity vulnerabilities.

Vulnerabilities	Severity	Status
Usage Of transfer Instead Of safeTransfer	HIGH	Fixed
moveFund function exposed	MEDIUM	Acknowledged
Integer Overflow	MEDIUM	Fixed
For Loop Over Dynamic Array	LOW	Acknowledged
Missing Address Verification	LOW	Fixed
Usage of block.timestamp	LOW	Acknowledged
Missing Address Verification	LOW	Fixed

3 Finding Details

A KommunitasProject.sol

A.1 Usage Of transfer Instead Of safeTransfer [HIGH]

Description:

The ERC20 standard token implementation functions also return the transaction status as a boolean. It is a good practice to check for the return status of the function call to ensure that the transaction was successful. It is the developer's responsibility to enclose these function calls with require() to ensure that, when the intended ERC20 function call returns false, the caller transaction also fails. However, it is mostly missed by developers when they carry out checks; in effect, the transaction would always succeed, even if the token transfer did not.

Code:

Listing 1: KommunitasProject.sol

```
1585 function moveFund() public {
1586     require(block.timestamp > booster[3].end, "Still in progress");
1587     if (payment.balanceOf(address(this)) > 0) {
1588         payment.transfer(factory.devAddr(),payment.balanceOf(address(
             ↪ this)));
1589     }
```

Risk Level:

Likelihood – 2

Impact - 5

Recommendation:

Use the safeTransfer function from the safeERC20 Implementation, or put the transfer call inside an assert or require verifying that it returned true.

Listing 2: KommunitasProject.sol

```
1585 function movefund() public {
1586     require(block.timestamp ? booster[3].end "still in progress");
1587     if (payment.balanceOf(address(this)) > 0 {
1588         require(payment.transfer(
1589             factory.devAddr(),
1590             payment.balanceOf(address(this))
1591         ),"Failed");
1592     }
1593     buyEnded = true;
1594 }
```

Status - Fixed

The Kommunitas team has resolved the issue by using safeTransfer function to remediate the risk.

A.2 moveFund function exposed [MEDIUM]

Description:

The moveFund function does not provide any functionalities to the users, the problem here is that anyone can call this function and drain the contract without having the approval from the Owner or the Developer.

Code:

Listing 3: KommunitasProject.sol

```
1585 function movefund() public {
1586     require(block.timestamp ? booster[3].end "still in progress");
```

```
1587        if (payment.balanceOf(address(this)) > 0 {
1588            require(payment.transfer(
1589                factory.devAddr(),
1590                payment.balanceOf(address(this))
1591            ),"Failed");
1592        }
1593        buyEnded = true;
1594    }
```

Risk Level:

Likelihood – 3
Impact - 3

Recommendation:

it is recommended to add a restriction in the call of the function using modifiers.

Status - Acknowledged

The Kommunitas team has acknowledged the risk.

A.3 Integer Overflow [MEDIUM]

Description:

Solidity versions that are below 0.8.0 does not have overflow protection, so if a variable is incremented after reaching the maximum value of its type, it will go back to zero.

Code:

Listing 4: KommunitasProject.sol

```
1229    for (uint256 i = 1; i <= 3; i++) {
1230        if (i == 1) {
1231        booster[i].start = _start;
```

```
1232      } else {
1233      booster[i].start = booster[i - 1].end + _boosterDelay;
1234      }
1235      booster[i].end = booster[i].start + _boosterRunning;
1236      booster[i].price = _price[i - 1].mul(10**payment.decimals()).div(
```

Listing 5: KommunitasProject.sol

```
1654  revenue += buyAmount;
1655  purchasePerRound[msg.sender][boosterProgress()] += tokenReceivedFinal;
1656  booster[boosterProgress()].achieve += tokenReceivedFinal;
1657  }
```

Recommendation:

It is recommended to use the SafeMath library to perform mathematical operations when using these versions.

Status - Fixed

The Kommunitas team has fixed the issue by using the SafeMath library to perform the mathematical operations.

A.4 For Loop Over Dynamic Array [LOW]

Description:

When smart contracts are deployed or their associated functions are invoked, the execution of these operations always consumes a certain quantity of gas, according to the amount of computation required to accomplish them. Modifying an unknown-size array that grows over time can result in a Denial-of-Service. Simply by having an excessively huge array, users can exceed the gas limit, therefore preventing the transaction from ever succeeding.

Code:

Listing 6: KommunitasProject.sol

```
1418 function whitelistTotalAlloc() public view returns (uint256 total) {
1419     total = 0;
1420         if (whitelists.length > 0) {
1421          for (uint256 i = 0; i < whitelists.length; i++) {
1422               total = total.add(whitelist[whitelists[i]]);
1423         }
1424     }
1425 }
```

Listing 7: KommunitasProject.sol

```
1871 function _swap(uint256[] memory amounts, address[] memory path, address
       ↪ _to) internal virtual {
1872     for (uint256 i; i < path.length - 1; i++) {
1873         (address input, address output) = (path[i], path[i + 1]);
1874         (address token0, ) = UniswapV2Library.sortTokens(input, output);
1875         uint256 amountOut = amounts[i + 1];
1876         (uint256 amount0Out, uint256 amount1Out) = input == token0
1877         ? (uint256(0), amountOut)
1878         : (amountOut, uint256(0));
1879         address to = i < path.length - 2
1880         ? UniswapV2Library.pairFor(factory.swapFactory(),output, path[i +
              ↪  2]): _to;
1881         IUniswapV2Pair(
1882         UniswapV2Library.pairFor(factory.swapFactory(), input, output)
1883         ).swap(amount0Out, amount1Out, to, new bytes(0));
1884     }
1885 }
```

Recommendation:

Avoid actions that involve looping across the entire data structure. If you really must loop over an array of unknown size, arrange for it to consume many blocs and thus multiple transactions.

Status - Acknowledged

The Kommunitas team has acknowledged the risk.

A.5 Missing Address Verification [LOW]

Description:

Certain functions lack a safety check in the address, the address-type argument should include a zero-address test, otherwise, the contract's functionality may become inaccessible.

Code:

Listing 8: KommunitasProject.sol

```
1199 function initialize(
1200     address _payment,
1201     address _adminProject,
1202     uint256 _tokenProjectDecimals,
1203     uint256 _sale,
1204     uint256 _target,
1205     uint256 _calculation,
1206     uint256 _start,
1207     uint256[3] memory _price,
1208     uint256[2] memory _minMaxPublicBuy,
1209     uint256 _tge,
1210     uint256 _boosterRunning,
1211     uint256 _boosterDelay
1212 ) public onlyFactory isNotInitialized {
1213     require(_boosterRunning > 0 && _boosterDelay > 0, "Can't be 0");
```

Listing 9: KommunitasProject.sol

```
1804 function setBuyer(address _user) internal returns (uint256 buyerId) {
1805     if (!isBuyer(_user)) {
1806         buyers.push(_user);
```

```
1807            buyerId = buyers.length - 1;

1809            bytes memory userRecipient = bytes(recipient[_user]);
1810            if (userRecipient.length == 0) {
1811                recipient[_user] = toAsciiString(_user);
1812            }
1813        } else {
1814            buyerId = invoices[_user][0].buyersIndex;
1815        }
1816    }
```

Listing 10: KommunitasProject.sol

```
1823        function setRecipient(string memory _recipient) public isNotPaused {
```

Risk Level:

Likelihood – 1
Impact - 3

Recommendation:

It's recommended to undertake further validation before user-supplied data. The concerns can be resolved by utilizing a whitelist technique or a modifier.

Status - Fixed

The Kommunitas team has fixed the issue by verifying the addresses provided in the arguments.

A.6 Usage of block.timestamp [LOW]

Description:

block.timestamp is used in the contract. The variable block is a set of variables. The timestamp does not always reflect the current time and may be inaccurate. The value of a block

can be influenced by miners. Maximal Extractable Value attacks require a timestamp of up to 900 seconds. There is no guarantee that the value is right, all that is guaranteed is that it is higher than the timestamp of the previous block.

Code:

Listing 11: KommunitasProject.sol

```
1155 modifier isBoosterProgress() {
1156     require(
1157         block.timestamp >= booster[boosterProgress()].start &&
1158             block.timestamp <= booster[boosterProgress()].end,
1159         "Not in any booster progress"
1160     );
1161     _;
1162 }
```

Listing 12: KommunitasProject.sol

```
1164 modifier ensure(uint256 deadline) {
1165     require(deadline >= block.timestamp, "UniswapV2Router: EXPIRED");
1166     _;
1167 }
```

Listing 13: KommunitasProject.sol

```
1393 function boosterProgress() public view returns (uint256 running) {
1394     running = 0;
1395     for (uint256 i = 1; i <= 3; i++) {
1396         if (
1397             block.timestamp >= booster[i].start &&
1398             block.timestamp <= booster[i].end
1399         ) {
1400             running = i;
1401         }
1402     }
1403 }
```

Listing 14: KommunitasProject.sol

```
1585 function movefund() public {
1586     require(block.timestamp ? booster[3].end "still in progress");
1587     if (payment.balanceOf(address(this)) > 0 {
1588         require(payment.transfer(
1589             factory.devAddr(),
1590             payment.balanceOf(address(this))
1591         ),"Failed");
1592     }
1593     buyEnded = true;
1594 }
```

Risk Level:

Likelihood – 1
Impact - 3

Recommendation:

Verify if a delay of 900 seconds will not impact the logic of the smart contract.

Status - Acknowledged

The Kommunitas team has acknowledged the risk.

B KommunitasFactory.sol

B.1 Missing Address Verification [LOW]

Description:

Certain functions lack a safety check in the address, the address-type argument should include a zero-address test, otherwise, the contract's functionality may become inaccessible.

Code:

Listing 15: KommunitasProject.sol

```
2028  constructor(address _swapFactory, address _weth, address _devAddr,
        ↪ address _savior, address _stakingV1, address _stakingV2){
2029      owner = msg.sender;
2030      swapFactory = _swapFactory;
2031      weth = _weth;
2032      devAddr = _devAddr;
2033      savior = _savior;
2034      stakingV1 = _stakingV1;
2035      stakingV2 = _stakingV2;
2036  }
```

Risk Level:

Likelihood – 1
Impact - 3

Recommendation:

It's recommended to undertake further validation before user-supplied data. The concerns can be resolved by utilizing a whitelist technique or a modifier.

Status - Fixed

The Kommunitas team has fixed the issue by verifying the addresses provided in the arguments.

4 Static Analysis (Slither)

Description:

ShellBoxes expanded the coverage of the specific contract areas using automated testing methodologies. Slither, a Solidity static analysis framework, was one of the tools used. Slither was run on all-scoped contracts in both text and binary formats. This tool can be used to test mathematical relationships between Solidity instances statically and variables that allow for the detection of errors or inconsistent usage of the contracts' APIs throughout the entire codebase.

Results:

```
Compilation warnings/errors on Launchpad_Core-main/KommunitasProject.sol
   ↪ :
Warning: Contract code size exceeds 24576 bytes (a limit introduced in
   ↪ Spurious Dragon). This contract may not be deployable on mainnet.
   ↪  Consider enabling the optimizer (with a low "runs" value!),
   ↪ turning off revert strings, or using libraries.
    --> Launchpad_Core-main/KommunitasProject.sol:1084:1:
     |
1084 | contract KommunitasProject {
     | ^ (Relevant source part starts here and spans across multiple
        ↪ lines).
```

```
Reentrancy in KommunitasProject.buyTokenByETH(address[]) (Launchpad_Core
   ↪ -main/KommunitasProject.sol#1600-1664):
      External calls:
      - IWETH(factory.weth()).deposit{value: ethFinal}() (
         ↪ Launchpad_Core-main/KommunitasProject.sol#1632)
      - TransferHelper.safeTransferETH(msg.sender,msg.value.sub(
         ↪ ethFinal)) (Launchpad_Core-main/KommunitasProject.sol
```

```
    ↪ #1635)
- buyAmount = swapToAccepted(ethFinal,_path,address(this)) (
    ↪ Launchpad_Core-main/KommunitasProject.sol#1638)
    - TransferHelper.safeTransferFrom(path[0],msg.sender,
        ↪ UniswapV2Library.pairFor(factory.swapFactory(),path
        ↪ [0],path[1]),amounts[0]) (Launchpad_Core-main/
        ↪ KommunitasProject.sol#1913-1918)
    - (success,data) = token.call(abi.encodeWithSelector(0
        ↪ x23b872dd,from,to,value)) (Launchpad_Core-main/
        ↪ KommunitasProject.sol#795-797)
    - assert(bool)(IWETH(factory.weth()).transfer(
        ↪ UniswapV2Library.pairFor(factory.swapFactory(),path
        ↪ [0],path[1]),amounts[0])) (Launchpad_Core-main/
        ↪ KommunitasProject.sol#1939-1948)
    - IUniswapV2Pair(UniswapV2Library.pairFor(factory.
        ↪ swapFactory(),input,output)).swap(amount0Out,
        ↪ amount1Out,to,new bytes(0)) (Launchpad_Core-main/
        ↪ KommunitasProject.sol#1891-1893)
External calls sending eth:
- IWETH(factory.weth()).deposit{value: ethFinal}() (
    ↪ Launchpad_Core-main/KommunitasProject.sol#1632)
State variables written after the call(s):
- booster[boosterProgress()].achieve += tokenReceivedFinal (
    ↪ Launchpad_Core-main/KommunitasProject.sol#1656)
- invoices[msg.sender].push(Invoice(buyerId,boosterProgress(),
    ↪ block.timestamp,buyAmount,tokenReceivedFinal)) (
    ↪ Launchpad_Core-main/KommunitasProject.sol#1644-1652)
- publicBought[msg.sender] = true (Launchpad_Core-main/
    ↪ KommunitasProject.sol#1641)
- purchasePerRound[msg.sender][boosterProgress()] +=
    ↪ tokenReceivedFinal (Launchpad_Core-main/KommunitasProject.
    ↪ sol#1655)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation
    ↪ #reentrancy-vulnerabilities
```

```
KommunitasProject.moveFund() (Launchpad_Core-main/KommunitasProject.sol
    ↪ #1585-1594) ignores return value by payment.transfer(factory.
    ↪ devAddr(),payment.balanceOf(address(this))) (Launchpad_Core-main/
    ↪ KommunitasProject.sol#1588-1591)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation
    ↪ #unchecked-transfer

KommunitasProject.amountInCalcInner(address,uint256,uint256) (
    ↪ Launchpad_Core-main/KommunitasProject.sol#1510-1557) performs a
    ↪ multiplication on the result of a division:
        -amountInFinal = (getUserAllocToken(_user).sub(purchasePerRound[
            ↪ _user][boosterProgress()])).mul(booster[boosterProgress()
            ↪ ].price).div(10 ** tokenProjectDecimals) (Launchpad_Core-
            ↪ main/KommunitasProject.sol#1530-1536)
        -tokenReceivedFinal = amountInFinal.mul(10 **
            ↪ tokenProjectDecimals).div(booster[boosterProgress()].price
            ↪ ) (Launchpad_Core-main/KommunitasProject.sol#1554-1556)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation
    ↪ #divide-before-multiply

Reentrancy in KommunitasProject.buyToken(uint256,address) (
    ↪ Launchpad_Core-main/KommunitasProject.sol#1740-1798):
        External calls:
        - TransferHelper.safeTransferFrom(address(payment),msg.sender,
            ↪ address(this),amountInFinal) (Launchpad_Core-main/
            ↪ KommunitasProject.sol#1767-1772)
        State variables written after the call(s):
        - booster[boosterProgress()].achieve += tokenReceivedFinal (
            ↪ Launchpad_Core-main/KommunitasProject.sol#1790)
        - invoices[msg.sender].push(Invoice(buyerId,boosterProgress(),
            ↪ block.timestamp,amountInFinal,tokenReceivedFinal)) (
            ↪ Launchpad_Core-main/KommunitasProject.sol#1778-1786)
```

```
        - publicBought[msg.sender] = true (Launchpad_Core-main/
            ↪ KommunitasProject.sol#1775)
        - purchasePerRound[msg.sender][boosterProgress()] +=
            ↪ tokenReceivedFinal (Launchpad_Core-main/KommunitasProject.
            ↪ sol#1789)
    Reentrancy in KommunitasProject.buyTokenByToken(uint256,address[]) (
        ↪ Launchpad_Core-main/KommunitasProject.sol#1671-1733):
        External calls:
        - buyAmount = swapToAccepted(_amountIn.mul(amountInFinal).div(
            ↪ amountOut),_path,address(this)) (Launchpad_Core-main/
            ↪ KommunitasProject.sol#1703-1707)
            - TransferHelper.safeTransferFrom(path[0],msg.sender,
                ↪ UniswapV2Library.pairFor(factory.swapFactory(),path
                ↪ [0],path[1]),amounts[0]) (Launchpad_Core-main/
                ↪ KommunitasProject.sol#1913-1918)
            - (success,data) = token.call(abi.encodeWithSelector(0
                ↪ x23b872dd,from,to,value)) (Launchpad_Core-main/
                ↪ KommunitasProject.sol#795-797)
            - assert(bool)(IWETH(factory.weth()).transfer(
                ↪ UniswapV2Library.pairFor(factory.swapFactory(),path
                ↪ [0],path[1]),amounts[0])) (Launchpad_Core-main/
                ↪ KommunitasProject.sol#1939-1948)
            - IUniswapV2Pair(UniswapV2Library.pairFor(factory.
                ↪ swapFactory(),input,output)).swap(amount0Out,
                ↪ amount1Out,to,new bytes(0)) (Launchpad_Core-main/
                ↪ KommunitasProject.sol#1891-1893)
        State variables written after the call(s):
        - booster[boosterProgress()].achieve += tokenReceivedFinal (
            ↪ Launchpad_Core-main/KommunitasProject.sol#1725)
        - invoices[msg.sender].push(Invoice(buyerId,boosterProgress(),
            ↪ block.timestamp,buyAmount,tokenReceivedFinal)) (
            ↪ Launchpad_Core-main/KommunitasProject.sol#1713-1721)
        - publicBought[msg.sender] = true (Launchpad_Core-main/
            ↪ KommunitasProject.sol#1710)
```

```
        - purchasePerRound[msg.sender][boosterProgress()] +=
            ↪ tokenReceivedFinal (Launchpad_Core-main/KommunitasProject.
            ↪ sol#1724)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation
    ↪ #reentrancy-vulnerabilities-1

UniswapV2Library.getAmountsOut(address,uint256,address[]).i (
    ↪ Launchpad_Core-main/KommunitasProject.sol#1052) is a local
    ↪ variable never initialized
KommunitasProject._swap(uint256[],address[],address).i (Launchpad_Core-
    ↪ main/KommunitasProject.sol#1876) is a local variable never
    ↪ initialized
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation
    ↪ #uninitialized-local-variables

KommunitasProject.transferOwnership(address) (Launchpad_Core-main/
    ↪ KommunitasProject.sol#2000-2003) should emit an event for:
        - owner = _newOwner (Launchpad_Core-main/KommunitasProject.sol
            ↪ #2002)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation
    ↪ #missing-events-access-control

KommunitasProject.initialize(address,address,uint256,uint256,uint256,
    ↪ uint256,uint256,uint256[3],uint256[2],uint256,uint256,uint256) (
    ↪ Launchpad_Core-main/KommunitasProject.sol#1199-1250) should emit
    ↪ an event for:
        - tokenProjectDecimals = _tokenProjectDecimals (Launchpad_Core-
            ↪ main/KommunitasProject.sol#1224)
        - sale = _sale (Launchpad_Core-main/KommunitasProject.sol#1225)
        - calculation = _calculation (Launchpad_Core-main/
            ↪ KommunitasProject.sol#1227)
        - minPublicBuy = _minMaxPublicBuy[0].mul(10 **
            ↪ tokenProjectDecimals) (Launchpad_Core-main/
            ↪ KommunitasProject.sol#1248)
```

```
        - maxPublicBuy = _minMaxPublicBuy[1].mul(10 **
            ↪ tokenProjectDecimals) (Launchpad_Core-main/
            ↪ KommunitasProject.sol#1249)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation
    ↪ #missing-events-arithmetic

KommunitasProject.initialize(address,address,uint256,uint256,uint256,
    ↪ uint256,uint256,uint256[3],uint256[2],uint256,uint256,uint256).
    ↪ _adminProject (Launchpad_Core-main/KommunitasProject.sol#1201)
    ↪ lacks a zero-check on :
                - adminProject = _adminProject (Launchpad_Core-main/
                    ↪ KommunitasProject.sol#1223)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation
    ↪ #missing-zero-address-validation

KommunitasProject.initialize(address,address,uint256,uint256,uint256,
    ↪ uint256,uint256,uint256[3],uint256[2],uint256,uint256,uint256) (
    ↪ Launchpad_Core-main/KommunitasProject.sol#1199-1250) has external
    ↪  calls inside a loop: booster[i].price = _price[i - 1].mul(10 **
    ↪ payment.decimals()).div(1e6) (Launchpad_Core-main/
    ↪ KommunitasProject.sol#1236-1238)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation
    ↪ /#calls-inside-a-loop

Reentrancy in KommunitasProject.buyToken(uint256,address) (
    ↪ Launchpad_Core-main/KommunitasProject.sol#1740-1798):
        External calls:
        - TransferHelper.safeTransferFrom(address(payment),msg.sender,
            ↪ address(this),amountInFinal) (Launchpad_Core-main/
            ↪ KommunitasProject.sol#1767-1772)
        State variables written after the call(s):
        - revenue += amountInFinal (Launchpad_Core-main/KommunitasProject
            ↪ .sol#1788)
```

```
Reentrancy in KommunitasProject.buyTokenByETH(address[]) (Launchpad_Core
    ↪ -main/KommunitasProject.sol#1600-1664):
        External calls:
        - IWETH(factory.weth()).deposit{value: ethFinal}() (
            ↪ Launchpad_Core-main/KommunitasProject.sol#1632)
        - TransferHelper.safeTransferETH(msg.sender,msg.value.sub(
            ↪ ethFinal)) (Launchpad_Core-main/KommunitasProject.sol
            ↪ #1635)
        - buyAmount = swapToAccepted(ethFinal,_path,address(this)) (
            ↪ Launchpad_Core-main/KommunitasProject.sol#1638)
                - TransferHelper.safeTransferFrom(path[0],msg.sender,
                    ↪ UniswapV2Library.pairFor(factory.swapFactory(),path
                    ↪ [0],path[1]),amounts[0]) (Launchpad_Core-main/
                    ↪ KommunitasProject.sol#1913-1918)
                - (success,data) = token.call(abi.encodeWithSelector(0
                    ↪ x23b872dd,from,to,value)) (Launchpad_Core-main/
                    ↪ KommunitasProject.sol#795-797)
                - assert(bool)(IWETH(factory.weth()).transfer(
                    ↪ UniswapV2Library.pairFor(factory.swapFactory(),path
                    ↪ [0],path[1]),amounts[0])) (Launchpad_Core-main/
                    ↪ KommunitasProject.sol#1939-1948)
                - IUniswapV2Pair(UniswapV2Library.pairFor(factory.
                    ↪ swapFactory(),input,output)).swap(amount0Out,
                    ↪ amount1Out,to,new bytes(0)) (Launchpad_Core-main/
                    ↪ KommunitasProject.sol#1891-1893)
        External calls sending eth:
        - IWETH(factory.weth()).deposit{value: ethFinal}() (
            ↪ Launchpad_Core-main/KommunitasProject.sol#1632)
        State variables written after the call(s):
        - revenue += buyAmount (Launchpad_Core-main/KommunitasProject.sol
            ↪ #1654)
Reentrancy in KommunitasProject.buyTokenByToken(uint256,address[]) (
    ↪ Launchpad_Core-main/KommunitasProject.sol#1671-1733):
        External calls:
```

```
        - buyAmount = swapToAccepted(_amountIn.mul(amountInFinal).div(
            ↪ amountOut),_path,address(this)) (Launchpad_Core-main/
            ↪ KommunitasProject.sol#1703-1707)
                - TransferHelper.safeTransferFrom(path[0],msg.sender,
                    ↪ UniswapV2Library.pairFor(factory.swapFactory(),path
                    ↪ [0],path[1]),amounts[0]) (Launchpad_Core-main/
                    ↪ KommunitasProject.sol#1913-1918)
                - (success,data) = token.call(abi.encodeWithSelector(0
                    ↪ x23b872dd,from,to,value)) (Launchpad_Core-main/
                    ↪ KommunitasProject.sol#795-797)
                - assert(bool)(IWETH(factory.weth()).transfer(
                    ↪ UniswapV2Library.pairFor(factory.swapFactory(),path
                    ↪ [0],path[1]),amounts[0])) (Launchpad_Core-main/
                    ↪ KommunitasProject.sol#1939-1948)
                - IUniswapV2Pair(UniswapV2Library.pairFor(factory.
                    ↪ swapFactory(),input,output)).swap(amount0Out,
                    ↪ amount1Out,to,new bytes(0)) (Launchpad_Core-main/
                    ↪ KommunitasProject.sol#1891-1893)
        State variables written after the call(s):
        - revenue += buyAmount (Launchpad_Core-main/KommunitasProject.sol
            ↪ #1723)
Reentrancy in KommunitasProject.moveFund() (Launchpad_Core-main/
    ↪ KommunitasProject.sol#1585-1594):
        External calls:
        - payment.transfer(factory.devAddr(),payment.balanceOf(address(
            ↪ this))) (Launchpad_Core-main/KommunitasProject.sol
            ↪ #1588-1591)
        State variables written after the call(s):
        - buyEnded = true (Launchpad_Core-main/KommunitasProject.sol
            ↪ #1593)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation
    ↪ #reentrancy-vulnerabilities-2
```

```
Reentrancy in KommunitasProject.buyToken(uint256,address) (
    ↪ Launchpad_Core-main/KommunitasProject.sol#1740-1798):
        External calls:
        - TransferHelper.safeTransferFrom(address(payment),msg.sender,
            ↪ address(this),amountInFinal) (Launchpad_Core-main/
            ↪ KommunitasProject.sol#1767-1772)
        Event emitted after the call(s):
        - TokenBought(boosterProgress(),msg.sender,amountInFinal,
            ↪ tokenReceivedFinal) (Launchpad_Core-main/KommunitasProject
            ↪ .sol#1792-1797)
Reentrancy in KommunitasProject.buyTokenByETH(address[]) (Launchpad_Core
    ↪ -main/KommunitasProject.sol#1600-1664):
        External calls:
        - IWETH(factory.weth()).deposit{value: ethFinal}() (
            ↪ Launchpad_Core-main/KommunitasProject.sol#1632)
        - TransferHelper.safeTransferETH(msg.sender,msg.value.sub(
            ↪ ethFinal)) (Launchpad_Core-main/KommunitasProject.sol
            ↪ #1635)
        - buyAmount = swapToAccepted(ethFinal,_path,address(this)) (
            ↪ Launchpad_Core-main/KommunitasProject.sol#1638)
                - TransferHelper.safeTransferFrom(path[0],msg.sender,
                    ↪ UniswapV2Library.pairFor(factory.swapFactory(),path
                    ↪ [0],path[1]),amounts[0]) (Launchpad_Core-main/
                    ↪ KommunitasProject.sol#1913-1918)
                - (success,data) = token.call(abi.encodeWithSelector(0
                    ↪ x23b872dd,from,to,value)) (Launchpad_Core-main/
                    ↪ KommunitasProject.sol#795-797)
                - assert(bool)(IWETH(factory.weth()).transfer(
                    ↪ UniswapV2Library.pairFor(factory.swapFactory(),path
                    ↪ [0],path[1]),amounts[0])) (Launchpad_Core-main/
                    ↪ KommunitasProject.sol#1939-1948)
                - IUniswapV2Pair(UniswapV2Library.pairFor(factory.
                    ↪ swapFactory(),input,output)).swap(amount0Out,
                    ↪ amount1Out,to,new bytes(0)) (Launchpad_Core-main/
```

```
                ↪ KommunitasProject.sol#1891-1893)
        External calls sending eth:
        - IWETH(factory.weth()).deposit{value: ethFinal}() (
            ↪ Launchpad_Core-main/KommunitasProject.sol#1632)
        Event emitted after the call(s):
        - TokenBought(boosterProgress(),msg.sender,buyAmount,
            ↪ tokenReceivedFinal) (Launchpad_Core-main/KommunitasProject
            ↪ .sol#1658-1663)
    Reentrancy in KommunitasProject.buyTokenByToken(uint256,address[]) (
        ↪ Launchpad_Core-main/KommunitasProject.sol#1671-1733):
        External calls:
        - buyAmount = swapToAccepted(_amountIn.mul(amountInFinal).div(
            ↪ amountOut),_path,address(this)) (Launchpad_Core-main/
            ↪ KommunitasProject.sol#1703-1707)
            - TransferHelper.safeTransferFrom(path[0],msg.sender,
                ↪ UniswapV2Library.pairFor(factory.swapFactory(),path
                ↪ [0],path[1]),amounts[0]) (Launchpad_Core-main/
                ↪ KommunitasProject.sol#1913-1918)
            - (success,data) = token.call(abi.encodeWithSelector(0
                ↪ x23b872dd,from,to,value)) (Launchpad_Core-main/
                ↪ KommunitasProject.sol#795-797)
            - assert(bool)(IWETH(factory.weth()).transfer(
                ↪ UniswapV2Library.pairFor(factory.swapFactory(),path
                ↪ [0],path[1]),amounts[0])) (Launchpad_Core-main/
                ↪ KommunitasProject.sol#1939-1948)
            - IUniswapV2Pair(UniswapV2Library.pairFor(factory.
                ↪ swapFactory(),input,output)).swap(amount0Out,
                ↪ amount1Out,to,new bytes(0)) (Launchpad_Core-main/
                ↪ KommunitasProject.sol#1891-1893)
        Event emitted after the call(s):
        - TokenBought(boosterProgress(),msg.sender,buyAmount,
            ↪ tokenReceivedFinal) (Launchpad_Core-main/KommunitasProject
            ↪ .sol#1727-1732)
```

```
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation
    ↪ #reentrancy-vulnerabilities-3

KommunitasProject.boosterProgress() (Launchpad_Core-main/
    ↪ KommunitasProject.sol#1393-1403) uses timestamp for comparisons
        Dangerous comparisons:
        - block.timestamp >= booster[i].start && block.timestamp <=
            ↪ booster[i].end (Launchpad_Core-main/KommunitasProject.sol
            ↪ #1397-1398)
KommunitasProject.moveFund() (Launchpad_Core-main/KommunitasProject.sol
    ↪ #1585-1594) uses timestamp for comparisons
        Dangerous comparisons:
        - require(bool,string)(block.timestamp > booster[3].end,Still in
            ↪ progress) (Launchpad_Core-main/KommunitasProject.sol#1586)
KommunitasProject.setWhitelist_d6(address[],uint256[]) (Launchpad_Core-
    ↪ main/KommunitasProject.sol#1959-1976) uses timestamp for
    ↪ comparisons
        Dangerous comparisons:
        - require(bool,string)(block.timestamp < calculation,Calculation
            ↪ has been started) (Launchpad_Core-main/KommunitasProject.
            ↪ sol#1963)
KommunitasProject.setV2Staked() (Launchpad_Core-main/KommunitasProject.
    ↪ sol#1990-1998) uses timestamp for comparisons
        Dangerous comparisons:
        - require(bool,string)(block.timestamp >= calculation,Calculation
            ↪  is not started yet) (Launchpad_Core-main/
            ↪ KommunitasProject.sol#1991-1994)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation
    ↪ #block-timestamp

Different versions of Solidity are used:
        - Version used: ['0.7.6', '>=0.5.0', '>=0.6.0', '^0.7.0']
        - ^0.7.0 (Launchpad_Core-main/KommunitasProject.sol#3)
        - ^0.7.0 (Launchpad_Core-main/KommunitasProject.sol#26)
```

```
        - ^0.7.0 (Launchpad_Core-main/KommunitasProject.sol#115)
        - ^0.7.0 (Launchpad_Core-main/KommunitasProject.sol#285)
        - 0.7.6 (Launchpad_Core-main/KommunitasProject.sol#650)
        - 0.7.6 (Launchpad_Core-main/KommunitasProject.sol#709)
        - 0.7.6 (Launchpad_Core-main/KommunitasProject.sol#717)
        - >=0.5.0 (Launchpad_Core-main/KommunitasProject.sol#744)
        - >=0.6.0 (Launchpad_Core-main/KommunitasProject.sol#754)
        - 0.7.6 (Launchpad_Core-main/KommunitasProject.sol#810)
        - 0.7.6 (Launchpad_Core-main/KommunitasProject.sol#842)
        - 0.7.6 (Launchpad_Core-main/KommunitasProject.sol#953)
        - 0.7.6 (Launchpad_Core-main/KommunitasProject.sol#1082)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation
    ↪ #different-pragma-directives-are-used

Context._msgData() (Launchpad_Core-main/KommunitasProject.sol#20-23) is
    ↪ never used and should be removed
ERC20._burn(address,uint256) (Launchpad_Core-main/KommunitasProject.sol
    ↪ #580-591) is never used and should be removed
ERC20._mint(address,uint256) (Launchpad_Core-main/KommunitasProject.sol
    ↪ #559-567) is never used and should be removed
ERC20._setupDecimals(uint8) (Launchpad_Core-main/KommunitasProject.sol
    ↪ #625-627) is never used and should be removed
SafeMath.mod(uint256,uint256) (Launchpad_Core-main/KommunitasProject.sol
    ↪ #259-261) is never used and should be removed
SafeMath.mod(uint256,uint256,string) (Launchpad_Core-main/
    ↪ KommunitasProject.sol#275-282) is never used and should be
    ↪ removed
TransferHelper.safeApprove(address,address,uint256) (Launchpad_Core-main
    ↪ /KommunitasProject.sol#758-771) is never used and should be
    ↪ removed
TransferHelper.safeTransfer(address,address,uint256) (Launchpad_Core-
    ↪ main/KommunitasProject.sol#773-786) is never used and should be
    ↪ removed
```

```
UniswapV2Library.getAmountIn(uint256,uint256,uint256) (Launchpad_Core-
    ↪ main/KommunitasProject.sol#1028-1041) is never used and should be
    ↪  removed
UniswapV2Library.getAmountsIn(address,uint256,address[]) (Launchpad_Core
    ↪ -main/KommunitasProject.sol#1063-1079) is never used and should
    ↪ be removed
UniswapV2Library.quote(uint256,uint256,uint256) (Launchpad_Core-main/
    ↪ KommunitasProject.sol#997-1008) is never used and should be
    ↪ removed
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation
    ↪ #dead-code

Pragma version^0.7.0 (Launchpad_Core-main/KommunitasProject.sol#3)
    ↪ allows old versions
Pragma version^0.7.0 (Launchpad_Core-main/KommunitasProject.sol#26)
    ↪ allows old versions
Pragma version^0.7.0 (Launchpad_Core-main/KommunitasProject.sol#115)
    ↪ allows old versions
Pragma version^0.7.0 (Launchpad_Core-main/KommunitasProject.sol#285)
    ↪ allows old versions
Pragma version>=0.5.0 (Launchpad_Core-main/KommunitasProject.sol#744)
    ↪ allows old versions
Pragma version>=0.6.0 (Launchpad_Core-main/KommunitasProject.sol#754)
    ↪ allows old versions
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation
    ↪ #incorrect-versions-of-solidity

Low level call in TransferHelper.safeApprove(address,address,uint256) (
    ↪ Launchpad_Core-main/KommunitasProject.sol#758-771):
        - (success,data) = token.call(abi.encodeWithSelector(0x095ea7b3,
            ↪ to,value)) (Launchpad_Core-main/KommunitasProject.sol
            ↪ #764-766)
Low level call in TransferHelper.safeTransfer(address,address,uint256) (
    ↪ Launchpad_Core-main/KommunitasProject.sol#773-786):
```

```
        - (success,data) = token.call(abi.encodeWithSelector(0xa9059cbb,
            ↪ to,value)) (Launchpad_Core-main/KommunitasProject.sol
            ↪ #779-781)
Low level call in TransferHelper.safeTransferFrom(address,address,
    ↪ address,uint256) (Launchpad_Core-main/KommunitasProject.sol
    ↪ #788-802):
        - (success,data) = token.call(abi.encodeWithSelector(0x23b872dd,
            ↪ from,to,value)) (Launchpad_Core-main/KommunitasProject.sol
            ↪ #795-797)
Low level call in TransferHelper.safeTransferETH(address,uint256) (
    ↪ Launchpad_Core-main/KommunitasProject.sol#804-807):
        - (success) = to.call{value: value}(new bytes(0)) (Launchpad_Core
            ↪ -main/KommunitasProject.sol#805)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation
    ↪ #low-level-calls

Function IUniswapV2Pair.DOMAIN_SEPARATOR() (Launchpad_Core-main/
    ↪ KommunitasProject.sol#877) is not in mixedCase
Function IUniswapV2Pair.PERMIT_TYPEHASH() (Launchpad_Core-main/
    ↪ KommunitasProject.sol#879) is not in mixedCase
Function IUniswapV2Pair.MINIMUM_LIQUIDITY() (Launchpad_Core-main/
    ↪ KommunitasProject.sol#910) is not in mixedCase
Parameter KommunitasProject.initialize(address,address,uint256,uint256,
    ↪ uint256,uint256,uint256,uint256[3],uint256[2],uint256,uint256,
    ↪ uint256)._payment (Launchpad_Core-main/KommunitasProject.sol
    ↪ #1200) is not in mixedCase
Parameter KommunitasProject.initialize(address,address,uint256,uint256,
    ↪ uint256,uint256,uint256,uint256[3],uint256[2],uint256,uint256,
    ↪ uint256)._adminProject (Launchpad_Core-main/KommunitasProject.sol
    ↪ #1201) is not in mixedCase
Parameter KommunitasProject.initialize(address,address,uint256,uint256,
    ↪ uint256,uint256,uint256,uint256[3],uint256[2],uint256,uint256,
    ↪ uint256)._tokenProjectDecimals (Launchpad_Core-main/
    ↪ KommunitasProject.sol#1202) is not in mixedCase
```

```
Parameter KommunitasProject.initialize(address,address,uint256,uint256,
    ↪ uint256,uint256,uint256,uint256[3],uint256[2],uint256,uint256,
    ↪ uint256)._sale (Launchpad_Core-main/KommunitasProject.sol#1203)
    ↪ is not in mixedCase
Parameter KommunitasProject.initialize(address,address,uint256,uint256,
    ↪ uint256,uint256,uint256,uint256[3],uint256[2],uint256,uint256,
    ↪ uint256)._target (Launchpad_Core-main/KommunitasProject.sol#1204)
    ↪  is not in mixedCase
Parameter KommunitasProject.initialize(address,address,uint256,uint256,
    ↪ uint256,uint256,uint256,uint256[3],uint256[2],uint256,uint256,
    ↪ uint256)._calculation (Launchpad_Core-main/KommunitasProject.sol
    ↪ #1205) is not in mixedCase
Parameter KommunitasProject.initialize(address,address,uint256,uint256,
    ↪ uint256,uint256,uint256,uint256[3],uint256[2],uint256,uint256,
    ↪ uint256)._start (Launchpad_Core-main/KommunitasProject.sol#1206)
    ↪ is not in mixedCase
Parameter KommunitasProject.initialize(address,address,uint256,uint256,
    ↪ uint256,uint256,uint256,uint256[3],uint256[2],uint256,uint256,
    ↪ uint256)._price (Launchpad_Core-main/KommunitasProject.sol#1207)
    ↪ is not in mixedCase
Parameter KommunitasProject.initialize(address,address,uint256,uint256,
    ↪ uint256,uint256,uint256,uint256[3],uint256[2],uint256,uint256,
    ↪ uint256)._minMaxPublicBuy (Launchpad_Core-main/KommunitasProject.
    ↪ sol#1208) is not in mixedCase
Parameter KommunitasProject.initialize(address,address,uint256,uint256,
    ↪ uint256,uint256,uint256,uint256[3],uint256[2],uint256,uint256,
    ↪ uint256)._tge (Launchpad_Core-main/KommunitasProject.sol#1209) is
    ↪  not in mixedCase
Parameter KommunitasProject.initialize(address,address,uint256,uint256,
    ↪ uint256,uint256,uint256,uint256[3],uint256[2],uint256,uint256,
    ↪ uint256)._boosterRunning (Launchpad_Core-main/KommunitasProject.
    ↪ sol#1210) is not in mixedCase
Parameter KommunitasProject.initialize(address,address,uint256,uint256,
    ↪ uint256,uint256,uint256,uint256[3],uint256[2],uint256,uint256,
```

```
    ↪ uint256)._boosterDelay (Launchpad_Core-main/KommunitasProject.sol
    ↪ #1211) is not in mixedCase
Parameter KommunitasProject.getBuyerHistoryLength(address)._buyer (
    ↪ Launchpad_Core-main/KommunitasProject.sol#1271) is not in
    ↪ mixedCase
Parameter KommunitasProject.getUserStakedInfo(KommunitasProject.
    ↪ StakingChoice,address)._choice (Launchpad_Core-main/
    ↪ KommunitasProject.sol#1299) is not in mixedCase
Parameter KommunitasProject.getUserStakedInfo(KommunitasProject.
    ↪ StakingChoice,address)._target (Launchpad_Core-main/
    ↪ KommunitasProject.sol#1299) is not in mixedCase
Function KommunitasProject.getUserAllocation_d8(address) (Launchpad_Core
    ↪ -main/KommunitasProject.sol#1329-1345) is not in mixedCase
Parameter KommunitasProject.getUserAllocation_d8(address)._target (
    ↪ Launchpad_Core-main/KommunitasProject.sol#1329) is not in
    ↪ mixedCase
Parameter KommunitasProject.isBuyer(address)._user (Launchpad_Core-main/
    ↪ KommunitasProject.sol#1351) is not in mixedCase
Parameter KommunitasProject.getAmountOut(address,uint256)._tokenIn (
    ↪ Launchpad_Core-main/KommunitasProject.sol#1361) is not in
    ↪ mixedCase
Parameter KommunitasProject.getAmountOut(address,uint256)._amountIn (
    ↪ Launchpad_Core-main/KommunitasProject.sol#1361) is not in
    ↪ mixedCase
Parameter KommunitasProject.getTotalPurchase(address)._user (
    ↪ Launchpad_Core-main/KommunitasProject.sol#1380) is not in
    ↪ mixedCase
Parameter KommunitasProject.getUserAllocToken(address)._user (
    ↪ Launchpad_Core-main/KommunitasProject.sol#1432) is not in
    ↪ mixedCase
Parameter KommunitasProject.amountInCalc(uint256,uint256,address).
    ↪ _tokenReceived (Launchpad_Core-main/KommunitasProject.sol#1466)
    ↪ is not in mixedCase
```

```
Parameter KommunitasProject.amountInCalc(uint256,uint256,address).
    ↪ _amountIn (Launchpad_Core-main/KommunitasProject.sol#1467) is not
    ↪  in mixedCase
Parameter KommunitasProject.amountInCalc(uint256,uint256,address)._user
    ↪ (Launchpad_Core-main/KommunitasProject.sol#1468) is not in
    ↪ mixedCase
Parameter KommunitasProject.amountInCalcInner(address,uint256,uint256).
    ↪ _user (Launchpad_Core-main/KommunitasProject.sol#1511) is not in
    ↪ mixedCase
Parameter KommunitasProject.amountInCalcInner(address,uint256,uint256).
    ↪ _tokenReceived (Launchpad_Core-main/KommunitasProject.sol#1512)
    ↪ is not in mixedCase
Parameter KommunitasProject.amountInCalcInner(address,uint256,uint256).
    ↪ _amountIn (Launchpad_Core-main/KommunitasProject.sol#1513) is not
    ↪  in mixedCase
Parameter KommunitasProject.buyTokenByETH(address[])._path (
    ↪ Launchpad_Core-main/KommunitasProject.sol#1600) is not in
    ↪ mixedCase
Parameter KommunitasProject.buyTokenByToken(uint256,address[])._amountIn
    ↪  (Launchpad_Core-main/KommunitasProject.sol#1671) is not in
    ↪ mixedCase
Parameter KommunitasProject.buyTokenByToken(uint256,address[])._path (
    ↪ Launchpad_Core-main/KommunitasProject.sol#1671) is not in
    ↪ mixedCase
Parameter KommunitasProject.buyToken(uint256,address)._amountIn (
    ↪ Launchpad_Core-main/KommunitasProject.sol#1740) is not in
    ↪ mixedCase
Parameter KommunitasProject.buyToken(uint256,address)._tokenIn (
    ↪ Launchpad_Core-main/KommunitasProject.sol#1740) is not in
    ↪ mixedCase
Parameter KommunitasProject.setBuyer(address)._user (Launchpad_Core-main
    ↪ /KommunitasProject.sol#1804) is not in mixedCase
Parameter KommunitasProject.setRecipient(string)._recipient (
    ↪ Launchpad_Core-main/KommunitasProject.sol#1823) is not in
```

```
    ↪ mixedCase
Parameter KommunitasProject.swapToAccepted(uint256,address[],address).
    ↪ _amountIn (Launchpad_Core-main/KommunitasProject.sol#1836) is not
    ↪  in mixedCase
Parameter KommunitasProject.swapToAccepted(uint256,address[],address).
    ↪ _path (Launchpad_Core-main/KommunitasProject.sol#1837) is not in
    ↪ mixedCase
Parameter KommunitasProject.swapToAccepted(uint256,address[],address).
    ↪ _to (Launchpad_Core-main/KommunitasProject.sol#1838) is not in
    ↪ mixedCase
Function KommunitasProject.setWhitelist_d6(address[],uint256[]) (
    ↪ Launchpad_Core-main/KommunitasProject.sol#1959-1976) is not in
    ↪ mixedCase
Parameter KommunitasProject.setWhitelist_d6(address[],uint256[])._user (
    ↪ Launchpad_Core-main/KommunitasProject.sol#1960) is not in
    ↪ mixedCase
Parameter KommunitasProject.setWhitelist_d6(address[],uint256[]).
    ↪ _allocation (Launchpad_Core-main/KommunitasProject.sol#1961) is
    ↪ not in mixedCase
Parameter KommunitasProject.setTge(uint256)._tge (Launchpad_Core-main/
    ↪ KommunitasProject.sol#1981) is not in mixedCase
Parameter KommunitasProject.transferOwnership(address)._newOwner (
    ↪ Launchpad_Core-main/KommunitasProject.sol#2000) is not in
    ↪ mixedCase
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation
    ↪ #conformance-to-solidity-naming-conventions

Redundant expression "this (Launchpad_Core-main/KommunitasProject.sol
    ↪ #21)" inContext (Launchpad_Core-main/KommunitasProject.sol#15-24)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation
    ↪ #redundant-statements

Variable KommunitasProject.getUserAllocation_d8(address).userV1Staked (
    ↪ Launchpad_Core-main/KommunitasProject.sol#1334) is too similar to
```

```
    ↪  KommunitasProject.getUserAllocation_d8(address).userV2Staked (
    ↪ Launchpad_Core-main/KommunitasProject.sol#1338)
Variable KommunitasProject.getUserAllocation_d8(address).v1TotalStaked (
    ↪ Launchpad_Core-main/KommunitasProject.sol#1334) is too similar to
    ↪  KommunitasProject.getUserAllocation_d8(address).v2TotalStaked (
    ↪ Launchpad_Core-main/KommunitasProject.sol#1338)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation
    ↪ #variable-names-are-too-similar

name() should be declared external:
        - ERC20.name() (Launchpad_Core-main/KommunitasProject.sol
            ↪ #342-344)
symbol() should be declared external:
        - ERC20.symbol() (Launchpad_Core-main/KommunitasProject.sol
            ↪ #350-352)
decimals() should be declared external:
        - ERC20.decimals() (Launchpad_Core-main/KommunitasProject.sol
            ↪ #367-369)
totalSupply() should be declared external:
        - ERC20.totalSupply() (Launchpad_Core-main/KommunitasProject.sol
            ↪ #374-376)
balanceOf(address) should be declared external:
        - ERC20.balanceOf(address) (Launchpad_Core-main/KommunitasProject
            ↪ .sol#381-383)
transfer(address,uint256) should be declared external:
        - ERC20.transfer(address,uint256) (Launchpad_Core-main/
            ↪ KommunitasProject.sol#393-401)
allowance(address,address) should be declared external:
        - ERC20.allowance(address,address) (Launchpad_Core-main/
            ↪ KommunitasProject.sol#406-414)
approve(address,uint256) should be declared external:
        - ERC20.approve(address,uint256) (Launchpad_Core-main/
            ↪ KommunitasProject.sol#423-431)
transferFrom(address,address,uint256) should be declared external:
```

```
        - ERC20.transferFrom(address,address,uint256) (Launchpad_Core-
            ↪ main/KommunitasProject.sol#446-461)
increaseAllowance(address,uint256) should be declared external:
        - ERC20.increaseAllowance(address,uint256) (Launchpad_Core-main/
            ↪ KommunitasProject.sol#475-486)
decreaseAllowance(address,uint256) should be declared external:
        - ERC20.decreaseAllowance(address,uint256) (Launchpad_Core-main/
            ↪ KommunitasProject.sol#502-516)
initialize(address,address,uint256,uint256,uint256,uint256,uint256,
    ↪ uint256[3],uint256[2],uint256,uint256,uint256) should be declared
    ↪  external:
        - KommunitasProject.initialize(address,address,uint256,uint256,
            ↪ uint256,uint256,uint256,uint256[3],uint256[2],uint256,
            ↪ uint256,uint256) (Launchpad_Core-main/KommunitasProject.
            ↪ sol#1199-1250)
getWhitelistLength() should be declared external:
        - KommunitasProject.getWhitelistLength() (Launchpad_Core-main/
            ↪ KommunitasProject.sol#1257-1259)
getBuyersLength() should be declared external:
        - KommunitasProject.getBuyersLength() (Launchpad_Core-main/
            ↪ KommunitasProject.sol#1264-1266)
getBuyerHistoryLength(address) should be declared external:
        - KommunitasProject.getBuyerHistoryLength(address) (
            ↪ Launchpad_Core-main/KommunitasProject.sol#1271-1277)
getTotalPurchase(address) should be declared external:
        - KommunitasProject.getTotalPurchase(address) (Launchpad_Core-
            ↪ main/KommunitasProject.sol#1380-1388)
moveFund() should be declared external:
        - KommunitasProject.moveFund() (Launchpad_Core-main/
            ↪ KommunitasProject.sol#1585-1594)
buyTokenByETH(address[]) should be declared external:
        - KommunitasProject.buyTokenByETH(address[]) (Launchpad_Core-main
            ↪ /KommunitasProject.sol#1600-1664)
buyTokenByToken(uint256,address[]) should be declared external:
```

```
        - KommunitasProject.buyTokenByToken(uint256,address[]) (
            ↪ Launchpad_Core-main/KommunitasProject.sol#1671-1733)
buyToken(uint256,address) should be declared external:
        - KommunitasProject.buyToken(uint256,address) (Launchpad_Core-
            ↪ main/KommunitasProject.sol#1740-1798)
setRecipient(string) should be declared external:
        - KommunitasProject.setRecipient(string) (Launchpad_Core-main/
            ↪ KommunitasProject.sol#1823-1827)
setWhitelist_d6(address[],uint256[]) should be declared external:
        - KommunitasProject.setWhitelist_d6(address[],uint256[]) (
            ↪ Launchpad_Core-main/KommunitasProject.sol#1959-1976)
setTge(uint256) should be declared external:
        - KommunitasProject.setTge(uint256) (Launchpad_Core-main/
            ↪ KommunitasProject.sol#1981-1985)
setV2Staked() should be declared external:
        - KommunitasProject.setV2Staked() (Launchpad_Core-main/
            ↪ KommunitasProject.sol#1990-1998)
transferOwnership(address) should be declared external:
        - KommunitasProject.transferOwnership(address) (Launchpad_Core-
            ↪ main/KommunitasProject.sol#2000-2003)
togglePause() should be declared external:
        - KommunitasProject.togglePause() (Launchpad_Core-main/
            ↪ KommunitasProject.sol#2005-2007)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation
    ↪ #public-function-that-could-be-declared-external
Launchpad_Core-main/KommunitasProject.sol analyzed (13 contracts with 78
    ↪  detectors), 119 result(s) found

Compilation warnings/errors on Launchpad_Core-main/KommunitasFactory.sol
    ↪ :
Warning: Contract code size exceeds 24576 bytes (a limit introduced in
    ↪ Spurious Dragon). This contract may not be deployable on mainnet.
    ↪  Consider enabling the optimizer (with a low "runs" value!),
    ↪ turning off revert strings, or using libraries.
```

```
    --> Launchpad_Core-main/KommunitasFactory.sol:1084:1:
     |
1084 | contract KommunitasProject {
     | ^ (Relevant source part starts here and spans across multiple
        ↪ lines).

Warning: Contract code size exceeds 24576 bytes (a limit introduced in
   ↪ Spurious Dragon). This contract may not be deployable on mainnet.
   ↪  Consider enabling the optimizer (with a low "runs" value!),
   ↪ turning off revert strings, or using libraries.
    --> Launchpad_Core-main/KommunitasFactory.sol:2004:1:
     |
2004 | contract KommunitasFactory is IKommunitasFactory {
     | ^ (Relevant source part starts here and spans across multiple
        ↪ lines).



Reentrancy in KommunitasProject.buyTokenByETH(address[]) (Launchpad_Core
   ↪ -main/KommunitasFactory.sol#1598-1662):
       External calls:
       - IWETH(factory.weth()).deposit{value: ethFinal}() (
          ↪ Launchpad_Core-main/KommunitasFactory.sol#1630)
       - TransferHelper.safeTransferETH(msg.sender,msg.value.sub(
          ↪ ethFinal)) (Launchpad_Core-main/KommunitasFactory.sol
          ↪ #1633)
       - buyAmount = swapToAccepted(ethFinal,_path,address(this)) (
          ↪ Launchpad_Core-main/KommunitasFactory.sol#1636)
           - (success,data) = token.call(abi.encodeWithSelector(0
              ↪ x23b872dd,from,to,value)) (Launchpad_Core-main/
              ↪ KommunitasFactory.sol#795-797)
           - TransferHelper.safeTransferFrom(path[0],msg.sender,
              ↪ UniswapV2Library.pairFor(factory.swapFactory(),path
              ↪ [0],path[1]),amounts[0]) (Launchpad_Core-main/
```

```
                    ↪ KommunitasFactory.sol#1907-1912)
                - assert(bool)(IWETH(factory.weth()).transfer(
                    ↪ UniswapV2Library.pairFor(factory.swapFactory(),path
                    ↪ [0],path[1]),amounts[0])) (Launchpad_Core-main/
                    ↪ KommunitasFactory.sol#1933-1942)
                - IUniswapV2Pair(UniswapV2Library.pairFor(factory.
                    ↪ swapFactory(),input,output)).swap(amount0Out,
                    ↪ amount1Out,to,new bytes(0)) (Launchpad_Core-main/
                    ↪ KommunitasFactory.sol#1885-1887)
        External calls sending eth:
        - IWETH(factory.weth()).deposit{value: ethFinal}() (
            ↪ Launchpad_Core-main/KommunitasFactory.sol#1630)
        State variables written after the call(s):
        - booster[boosterProgress()].achieve += tokenReceivedFinal (
            ↪ Launchpad_Core-main/KommunitasFactory.sol#1654)
        - invoices[msg.sender].push(Invoice(buyerId,boosterProgress(),
            ↪ block.timestamp,buyAmount,tokenReceivedFinal)) (
            ↪ Launchpad_Core-main/KommunitasFactory.sol#1642-1650)
        - publicBought[msg.sender] = true (Launchpad_Core-main/
            ↪ KommunitasFactory.sol#1639)
        - purchasePerRound[msg.sender][boosterProgress()] +=
            ↪ tokenReceivedFinal (Launchpad_Core-main/KommunitasFactory.
            ↪ sol#1653)
    Reference: https://github.com/crytic/slither/wiki/Detector-Documentation
        ↪ #reentrancy-vulnerabilities

    KommunitasProject.moveFund() (Launchpad_Core-main/KommunitasFactory.sol
        ↪ #1583-1592) ignores return value by payment.transfer(factory.
        ↪ devAddr(),payment.balanceOf(address(this))) (Launchpad_Core-main/
        ↪ KommunitasFactory.sol#1586-1589)
    Reference: https://github.com/crytic/slither/wiki/Detector-Documentation
        ↪ #unchecked-transfer
```

```
KommunitasProject.amountInCalcInner(address,uint256,uint256) (
    ↪ Launchpad_Core-main/KommunitasFactory.sol#1508-1555) performs a
    ↪ multiplication on the result of a division:
        -amountInFinal = (getUserAllocToken(_user).sub(purchasePerRound[
            ↪ _user][boosterProgress()])).mul(booster[boosterProgress()
            ↪ ].price).div(10 ** tokenProjectDecimals) (Launchpad_Core-
            ↪ main/KommunitasFactory.sol#1528-1534)
        -tokenReceivedFinal = amountInFinal.mul(10 **
            ↪ tokenProjectDecimals).div(booster[boosterProgress()].price
            ↪ ) (Launchpad_Core-main/KommunitasFactory.sol#1552-1554)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation
    ↪ #divide-before-multiply

Reentrancy in KommunitasProject.buyToken(uint256,address) (
    ↪ Launchpad_Core-main/KommunitasFactory.sol#1738-1796):
        External calls:
        - TransferHelper.safeTransferFrom(address(payment),msg.sender,
            ↪ address(this),amountInFinal) (Launchpad_Core-main/
            ↪ KommunitasFactory.sol#1765-1770)
        State variables written after the call(s):
        - booster[boosterProgress()].achieve += tokenReceivedFinal (
            ↪ Launchpad_Core-main/KommunitasFactory.sol#1788)
        - invoices[msg.sender].push(Invoice(buyerId,boosterProgress(),
            ↪ block.timestamp,amountInFinal,tokenReceivedFinal)) (
            ↪ Launchpad_Core-main/KommunitasFactory.sol#1776-1784)
        - publicBought[msg.sender] = true (Launchpad_Core-main/
            ↪ KommunitasFactory.sol#1773)
        - purchasePerRound[msg.sender][boosterProgress()] +=
            ↪ tokenReceivedFinal (Launchpad_Core-main/KommunitasFactory.
            ↪ sol#1787)
Reentrancy in KommunitasProject.buyTokenByToken(uint256,address[]) (
    ↪ Launchpad_Core-main/KommunitasFactory.sol#1669-1731):
        External calls:
```

```
        - buyAmount = swapToAccepted(_amountIn.mul(amountInFinal).div(
            ↪ amountOut),_path,address(this)) (Launchpad_Core-main/
            ↪ KommunitasFactory.sol#1701-1705)
                - (success,data) = token.call(abi.encodeWithSelector(0
                    ↪ x23b872dd,from,to,value)) (Launchpad_Core-main/
                    ↪ KommunitasFactory.sol#795-797)
                - TransferHelper.safeTransferFrom(path[0],msg.sender,
                    ↪ UniswapV2Library.pairFor(factory.swapFactory(),path
                    ↪ [0],path[1]),amounts[0]) (Launchpad_Core-main/
                    ↪ KommunitasFactory.sol#1907-1912)
                - assert(bool)(IWETH(factory.weth()).transfer(
                    ↪ UniswapV2Library.pairFor(factory.swapFactory(),path
                    ↪ [0],path[1]),amounts[0])) (Launchpad_Core-main/
                    ↪ KommunitasFactory.sol#1933-1942)
                - IUniswapV2Pair(UniswapV2Library.pairFor(factory.
                    ↪ swapFactory(),input,output)).swap(amount0Out,
                    ↪ amount1Out,to,new bytes(0)) (Launchpad_Core-main/
                    ↪ KommunitasFactory.sol#1885-1887)
        State variables written after the call(s):
        - booster[boosterProgress()].achieve += tokenReceivedFinal (
            ↪ Launchpad_Core-main/KommunitasFactory.sol#1723)
        - invoices[msg.sender].push(Invoice(buyerId,boosterProgress(),
            ↪ block.timestamp,buyAmount,tokenReceivedFinal)) (
            ↪ Launchpad_Core-main/KommunitasFactory.sol#1711-1719)
        - publicBought[msg.sender] = true (Launchpad_Core-main/
            ↪ KommunitasFactory.sol#1708)
        - purchasePerRound[msg.sender][boosterProgress()] +=
            ↪ tokenReceivedFinal (Launchpad_Core-main/KommunitasFactory.
            ↪ sol#1722)
    Reference: https://github.com/crytic/slither/wiki/Detector-Documentation
        ↪ #reentrancy-vulnerabilities-1

    UniswapV2Library.getAmountsOut(address,uint256,address[]).i (
        ↪ Launchpad_Core-main/KommunitasFactory.sol#1052) is a local
```

```
    ↪ variable never initialized
KommunitasProject._swap(uint256[],address[],address).i (Launchpad_Core-
    ↪ main/KommunitasFactory.sol#1871) is a local variable never
    ↪ initialized
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation
    ↪ #uninitialized-local-variables

KommunitasProject.transferOwnership(address) (Launchpad_Core-main/
    ↪ KommunitasFactory.sol#1992-1995) should emit an event for:
        - owner = _newOwner (Launchpad_Core-main/KommunitasFactory.sol
            ↪ #1994)
KommunitasFactory.transferOwnership(address) (Launchpad_Core-main/
    ↪ KommunitasFactory.sol#2128-2131) should emit an event for:
        - owner = _newOwner (Launchpad_Core-main/KommunitasFactory.sol
            ↪ #2130)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation
    ↪ #missing-events-access-control

KommunitasProject.initialize(address,address,uint256,uint256,uint256,
    ↪ uint256,uint256,uint256[3],uint256[2],uint256,uint256,uint256) (
    ↪ Launchpad_Core-main/KommunitasFactory.sol#1199-1249) should emit
    ↪ an event for:
        - tokenProjectDecimals = _tokenProjectDecimals (Launchpad_Core-
            ↪ main/KommunitasFactory.sol#1223)
        - sale = _sale (Launchpad_Core-main/KommunitasFactory.sol#1224)
        - calculation = _calculation (Launchpad_Core-main/
            ↪ KommunitasFactory.sol#1226)
        - minPublicBuy = _minMaxPublicBuy[0].mul(10 **
            ↪ tokenProjectDecimals) (Launchpad_Core-main/
            ↪ KommunitasFactory.sol#1247)
        - maxPublicBuy = _minMaxPublicBuy[1].mul(10 **
            ↪ tokenProjectDecimals) (Launchpad_Core-main/
            ↪ KommunitasFactory.sol#1248)
```

```
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation
    ↪ #missing-events-arithmetic

KommunitasProject.initialize(address,address,uint256,uint256,uint256,
    ↪ uint256,uint256,uint256[3],uint256[2],uint256,uint256,uint256).
    ↪ _adminProject (Launchpad_Core-main/KommunitasFactory.sol#1201)
    ↪ lacks a zero-check on :
                - adminProject = _adminProject (Launchpad_Core-main/
                    ↪ KommunitasFactory.sol#1222)
KommunitasFactory.constructor(address,address,address,address,address).
    ↪ _swapFactory (Launchpad_Core-main/KommunitasFactory.sol#2029)
    ↪ lacks a zero-check on :
                - swapFactory = _swapFactory (Launchpad_Core-main/
                    ↪ KommunitasFactory.sol#2037)
KommunitasFactory.constructor(address,address,address,address,address).
    ↪ _weth (Launchpad_Core-main/KommunitasFactory.sol#2030) lacks a
    ↪ zero-check on :
                - weth = _weth (Launchpad_Core-main/KommunitasFactory.sol
                    ↪ #2038)
KommunitasFactory.constructor(address,address,address,address,address).
    ↪ _devAddr (Launchpad_Core-main/KommunitasFactory.sol#2031) lacks a
    ↪  zero-check on :
                - devAddr = _devAddr (Launchpad_Core-main/
                    ↪ KommunitasFactory.sol#2039)
KommunitasFactory.constructor(address,address,address,address,address).
    ↪ _stakingV1 (Launchpad_Core-main/KommunitasFactory.sol#2032) lacks
    ↪  a zero-check on :
                - stakingV1 = _stakingV1 (Launchpad_Core-main/
                    ↪ KommunitasFactory.sol#2040)
KommunitasFactory.constructor(address,address,address,address,address).
    ↪ _stakingV2 (Launchpad_Core-main/KommunitasFactory.sol#2033) lacks
    ↪  a zero-check on :
                - stakingV2 = _stakingV2 (Launchpad_Core-main/
                    ↪ KommunitasFactory.sol#2041)
```

```
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation
    ↪ #missing-zero-address-validation

KommunitasProject.initialize(address,address,uint256,uint256,uint256,
    ↪ uint256,uint256,uint256[3],uint256[2],uint256,uint256,uint256) (
    ↪ Launchpad_Core-main/KommunitasFactory.sol#1199-1249) has external
    ↪  calls inside a loop: booster[i].price = _price[i - 1].mul(10 **
    ↪ payment.decimals()).div(1e6) (Launchpad_Core-main/
    ↪ KommunitasFactory.sol#1235-1237)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation
    ↪ /#calls-inside-a-loop

Reentrancy in KommunitasProject.buyToken(uint256,address) (
    ↪ Launchpad_Core-main/KommunitasFactory.sol#1738-1796):
        External calls:
        - TransferHelper.safeTransferFrom(address(payment),msg.sender,
            ↪ address(this),amountInFinal) (Launchpad_Core-main/
            ↪ KommunitasFactory.sol#1765-1770)
        State variables written after the call(s):
        - revenue += amountInFinal (Launchpad_Core-main/KommunitasFactory
            ↪ .sol#1786)
Reentrancy in KommunitasProject.buyTokenByETH(address[]) (Launchpad_Core
    ↪ -main/KommunitasFactory.sol#1598-1662):
        External calls:
        - IWETH(factory.weth()).deposit{value: ethFinal}() (
            ↪ Launchpad_Core-main/KommunitasFactory.sol#1630)
        - TransferHelper.safeTransferETH(msg.sender,msg.value.sub(
            ↪ ethFinal)) (Launchpad_Core-main/KommunitasFactory.sol
            ↪ #1633)
        - buyAmount = swapToAccepted(ethFinal,_path,address(this)) (
            ↪ Launchpad_Core-main/KommunitasFactory.sol#1636)
                - (success,data) = token.call(abi.encodeWithSelector(0
                    ↪ x23b872dd,from,to,value)) (Launchpad_Core-main/
                    ↪ KommunitasFactory.sol#795-797)
```

```
            - TransferHelper.safeTransferFrom(path[0],msg.sender,
                ↪ UniswapV2Library.pairFor(factory.swapFactory(),path
                ↪ [0],path[1]),amounts[0]) (Launchpad_Core-main/
                ↪ KommunitasFactory.sol#1907-1912)
            - assert(bool)(IWETH(factory.weth()).transfer(
                ↪ UniswapV2Library.pairFor(factory.swapFactory(),path
                ↪ [0],path[1]),amounts[0])) (Launchpad_Core-main/
                ↪ KommunitasFactory.sol#1933-1942)
            - IUniswapV2Pair(UniswapV2Library.pairFor(factory.
                ↪ swapFactory(),input,output)).swap(amount0Out,
                ↪ amount1Out,to,new bytes(0)) (Launchpad_Core-main/
                ↪ KommunitasFactory.sol#1885-1887)
        External calls sending eth:
        - IWETH(factory.weth()).deposit{value: ethFinal}() (
            ↪ Launchpad_Core-main/KommunitasFactory.sol#1630)
        State variables written after the call(s):
        - revenue += buyAmount (Launchpad_Core-main/KommunitasFactory.sol
            ↪ #1652)
Reentrancy in KommunitasProject.buyTokenByToken(uint256,address[]) (
    ↪ Launchpad_Core-main/KommunitasFactory.sol#1669-1731):
        External calls:
        - buyAmount = swapToAccepted(_amountIn.mul(amountInFinal).div(
            ↪ amountOut),_path,address(this)) (Launchpad_Core-main/
            ↪ KommunitasFactory.sol#1701-1705)
            - (success,data) = token.call(abi.encodeWithSelector(0
                ↪ x23b872dd,from,to,value)) (Launchpad_Core-main/
                ↪ KommunitasFactory.sol#795-797)
            - TransferHelper.safeTransferFrom(path[0],msg.sender,
                ↪ UniswapV2Library.pairFor(factory.swapFactory(),path
                ↪ [0],path[1]),amounts[0]) (Launchpad_Core-main/
                ↪ KommunitasFactory.sol#1907-1912)
            - assert(bool)(IWETH(factory.weth()).transfer(
                ↪ UniswapV2Library.pairFor(factory.swapFactory(),path
                ↪ [0],path[1]),amounts[0])) (Launchpad_Core-main/
```

```
                    ↪ KommunitasFactory.sol#1933-1942)
                - IUniswapV2Pair(UniswapV2Library.pairFor(factory.
                    ↪ swapFactory(),input,output)).swap(amount0Out,
                    ↪ amount1Out,to,new bytes(0)) (Launchpad_Core-main/
                    ↪ KommunitasFactory.sol#1885-1887)
        State variables written after the call(s):
        - revenue += buyAmount (Launchpad_Core-main/KommunitasFactory.sol
            ↪ #1721)
Reentrancy in KommunitasProject.moveFund() (Launchpad_Core-main/
    ↪ KommunitasFactory.sol#1583-1592):
        External calls:
        - payment.transfer(factory.devAddr(),payment.balanceOf(address(
            ↪ this))) (Launchpad_Core-main/KommunitasFactory.sol
            ↪ #1586-1589)
        State variables written after the call(s):
        - buyEnded = true (Launchpad_Core-main/KommunitasFactory.sol
            ↪ #1591)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation
    ↪ #reentrancy-vulnerabilities-2

Reentrancy in KommunitasProject.buyToken(uint256,address) (
    ↪ Launchpad_Core-main/KommunitasFactory.sol#1738-1796):
        External calls:
        - TransferHelper.safeTransferFrom(address(payment),msg.sender,
            ↪ address(this),amountInFinal) (Launchpad_Core-main/
            ↪ KommunitasFactory.sol#1765-1770)
        Event emitted after the call(s):
        - TokenBought(boosterProgress(),msg.sender,amountInFinal,
            ↪ tokenReceivedFinal) (Launchpad_Core-main/KommunitasFactory
            ↪ .sol#1790-1795)
Reentrancy in KommunitasProject.buyTokenByETH(address[]) (Launchpad_Core
    ↪ -main/KommunitasFactory.sol#1598-1662):
        External calls:
```

```
        - IWETH(factory.weth()).deposit{value: ethFinal}() (
            ↪ Launchpad_Core-main/KommunitasFactory.sol#1630)
        - TransferHelper.safeTransferETH(msg.sender,msg.value.sub(
            ↪ ethFinal)) (Launchpad_Core-main/KommunitasFactory.sol
            ↪ #1633)
        - buyAmount = swapToAccepted(ethFinal,_path,address(this)) (
            ↪ Launchpad_Core-main/KommunitasFactory.sol#1636)
            - (success,data) = token.call(abi.encodeWithSelector(0
                ↪ x23b872dd,from,to,value)) (Launchpad_Core-main/
                ↪ KommunitasFactory.sol#795-797)
            - TransferHelper.safeTransferFrom(path[0],msg.sender,
                ↪ UniswapV2Library.pairFor(factory.swapFactory(),path
                ↪ [0],path[1]),amounts[0]) (Launchpad_Core-main/
                ↪ KommunitasFactory.sol#1907-1912)
            - assert(bool)(IWETH(factory.weth()).transfer(
                ↪ UniswapV2Library.pairFor(factory.swapFactory(),path
                ↪ [0],path[1]),amounts[0])) (Launchpad_Core-main/
                ↪ KommunitasFactory.sol#1933-1942)
            - IUniswapV2Pair(UniswapV2Library.pairFor(factory.
                ↪ swapFactory(),input,output)).swap(amount0Out,
                ↪ amount1Out,to,new bytes(0)) (Launchpad_Core-main/
                ↪ KommunitasFactory.sol#1885-1887)
        External calls sending eth:
        - IWETH(factory.weth()).deposit{value: ethFinal}() (
            ↪ Launchpad_Core-main/KommunitasFactory.sol#1630)
        Event emitted after the call(s):
        - TokenBought(boosterProgress(),msg.sender,buyAmount,
            ↪ tokenReceivedFinal) (Launchpad_Core-main/KommunitasFactory
            ↪ .sol#1656-1661)
    Reentrancy in KommunitasProject.buyTokenByToken(uint256,address[]) (
        ↪ Launchpad_Core-main/KommunitasFactory.sol#1669-1731):
        External calls:
        - buyAmount = swapToAccepted(_amountIn.mul(amountInFinal).div(
            ↪ amountOut),_path,address(this)) (Launchpad_Core-main/
```

```
        ↪ KommunitasFactory.sol#1701-1705)
            - (success,data) = token.call(abi.encodeWithSelector(0
              ↪ x23b872dd,from,to,value)) (Launchpad_Core-main/
              ↪ KommunitasFactory.sol#795-797)
            - TransferHelper.safeTransferFrom(path[0],msg.sender,
              ↪ UniswapV2Library.pairFor(factory.swapFactory(),path
              ↪ [0],path[1]),amounts[0]) (Launchpad_Core-main/
              ↪ KommunitasFactory.sol#1907-1912)
            - assert(bool)(IWETH(factory.weth()).transfer(
              ↪ UniswapV2Library.pairFor(factory.swapFactory(),path
              ↪ [0],path[1]),amounts[0])) (Launchpad_Core-main/
              ↪ KommunitasFactory.sol#1933-1942)
            - IUniswapV2Pair(UniswapV2Library.pairFor(factory.
              ↪ swapFactory(),input,output)).swap(amount0Out,
              ↪ amount1Out,to,new bytes(0)) (Launchpad_Core-main/
              ↪ KommunitasFactory.sol#1885-1887)
        Event emitted after the call(s):
        - TokenBought(boosterProgress(),msg.sender,buyAmount,
          ↪ tokenReceivedFinal) (Launchpad_Core-main/KommunitasFactory
          ↪ .sol#1725-1730)
Reentrancy in KommunitasFactory.createProject(address,address,uint256,
    ↪ uint256,uint256,uint256,uint256,uint256[3],uint256[2],uint256,
    ↪ uint256,uint256) (Launchpad_Core-main/KommunitasFactory.sol
    ↪ #2073-2122):
        External calls:
        - KommunitasProject(getProject[_adminProject]).initialize(
          ↪ _payment,_adminProject,_tokenProjectDecimals,_sale,_target
          ↪ ,_calculation,_start,_price,_minMaxPublicBuy,_tge,
          ↪ _boosterRunning,_boosterDelay) (Launchpad_Core-main/
          ↪ KommunitasFactory.sol#2106-2119)
        Event emitted after the call(s):
        - ProjectCreated(_adminProject,project,allProjects.length - 1) (
          ↪ Launchpad_Core-main/KommunitasFactory.sol#2121)
```

```
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation
    ↪ #reentrancy-vulnerabilities-3

KommunitasProject.boosterProgress() (Launchpad_Core-main/
    ↪ KommunitasFactory.sol#1392-1402) uses timestamp for comparisons
        Dangerous comparisons:
        - block.timestamp >= booster[i].start && block.timestamp <=
            ↪ booster[i].end (Launchpad_Core-main/KommunitasFactory.sol
            ↪ #1396-1397)
KommunitasProject.moveFund() (Launchpad_Core-main/KommunitasFactory.sol
    ↪ #1583-1592) uses timestamp for comparisons
        Dangerous comparisons:
        - require(bool,string)(block.timestamp > booster[3].end,Still in
            ↪ progress) (Launchpad_Core-main/KommunitasFactory.sol#1584)
KommunitasProject.setWhitelist_d6(address[],uint256[]) (Launchpad_Core-
    ↪ main/KommunitasFactory.sol#1953-1969) uses timestamp for
    ↪ comparisons
        Dangerous comparisons:
        - require(bool,string)(block.timestamp < calculation,Calculation
            ↪ has been started) (Launchpad_Core-main/KommunitasFactory.
            ↪ sol#1957)
KommunitasProject.setV2Staked() (Launchpad_Core-main/KommunitasFactory.
    ↪ sol#1982-1990) uses timestamp for comparisons
        Dangerous comparisons:
        - require(bool,string)(block.timestamp >= calculation,Calculation
            ↪  is not started yet) (Launchpad_Core-main/
            ↪ KommunitasFactory.sol#1983-1986)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation
    ↪ #block-timestamp

Different versions of Solidity are used:
        - Version used: ['0.7.6', '>=0.5.0', '>=0.6.0', '^0.7.0']
        - ^0.7.0 (Launchpad_Core-main/KommunitasFactory.sol#3)
        - ^0.7.0 (Launchpad_Core-main/KommunitasFactory.sol#26)
```

```
        - ^0.7.0 (Launchpad_Core-main/KommunitasFactory.sol#115)
        - ^0.7.0 (Launchpad_Core-main/KommunitasFactory.sol#285)
        - 0.7.6 (Launchpad_Core-main/KommunitasFactory.sol#650)
        - 0.7.6 (Launchpad_Core-main/KommunitasFactory.sol#709)
        - 0.7.6 (Launchpad_Core-main/KommunitasFactory.sol#717)
        - >=0.5.0 (Launchpad_Core-main/KommunitasFactory.sol#744)
        - >=0.6.0 (Launchpad_Core-main/KommunitasFactory.sol#754)
        - 0.7.6 (Launchpad_Core-main/KommunitasFactory.sol#810)
        - 0.7.6 (Launchpad_Core-main/KommunitasFactory.sol#842)
        - 0.7.6 (Launchpad_Core-main/KommunitasFactory.sol#953)
        - 0.7.6 (Launchpad_Core-main/KommunitasFactory.sol#1082)
        - 0.7.6 (Launchpad_Core-main/KommunitasFactory.sol#2002)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation
    ↪ #different-pragma-directives-are-used

Context._msgData() (Launchpad_Core-main/KommunitasFactory.sol#20-23) is
    ↪ never used and should be removed
ERC20._burn(address,uint256) (Launchpad_Core-main/KommunitasFactory.sol
    ↪ #580-591) is never used and should be removed
ERC20._mint(address,uint256) (Launchpad_Core-main/KommunitasFactory.sol
    ↪ #559-567) is never used and should be removed
ERC20._setupDecimals(uint8) (Launchpad_Core-main/KommunitasFactory.sol
    ↪ #625-627) is never used and should be removed
SafeMath.mod(uint256,uint256) (Launchpad_Core-main/KommunitasFactory.sol
    ↪ #259-261) is never used and should be removed
SafeMath.mod(uint256,uint256,string) (Launchpad_Core-main/
    ↪ KommunitasFactory.sol#275-282) is never used and should be
    ↪ removed
TransferHelper.safeApprove(address,address,uint256) (Launchpad_Core-main
    ↪ /KommunitasFactory.sol#758-771) is never used and should be
    ↪ removed
TransferHelper.safeTransfer(address,address,uint256) (Launchpad_Core-
    ↪ main/KommunitasFactory.sol#773-786) is never used and should be
    ↪ removed
```

```
UniswapV2Library.getAmountIn(uint256,uint256,uint256) (Launchpad_Core-
    ↪ main/KommunitasFactory.sol#1028-1041) is never used and should be
    ↪  removed
UniswapV2Library.getAmountsIn(address,uint256,address[]) (Launchpad_Core
    ↪ -main/KommunitasFactory.sol#1063-1079) is never used and should
    ↪ be removed
UniswapV2Library.quote(uint256,uint256,uint256) (Launchpad_Core-main/
    ↪ KommunitasFactory.sol#997-1008) is never used and should be
    ↪ removed
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation
    ↪ #dead-code

Pragma version^0.7.0 (Launchpad_Core-main/KommunitasFactory.sol#3)
    ↪ allows old versions
Pragma version^0.7.0 (Launchpad_Core-main/KommunitasFactory.sol#26)
    ↪ allows old versions
Pragma version^0.7.0 (Launchpad_Core-main/KommunitasFactory.sol#115)
    ↪ allows old versions
Pragma version^0.7.0 (Launchpad_Core-main/KommunitasFactory.sol#285)
    ↪ allows old versions
Pragma version>=0.5.0 (Launchpad_Core-main/KommunitasFactory.sol#744)
    ↪ allows old versions
Pragma version>=0.6.0 (Launchpad_Core-main/KommunitasFactory.sol#754)
    ↪ allows old versions
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation
    ↪ #incorrect-versions-of-solidity

Low level call in TransferHelper.safeApprove(address,address,uint256) (
    ↪ Launchpad_Core-main/KommunitasFactory.sol#758-771):
        - (success,data) = token.call(abi.encodeWithSelector(0x095ea7b3,
            ↪ to,value)) (Launchpad_Core-main/KommunitasFactory.sol
            ↪ #764-766)
Low level call in TransferHelper.safeTransfer(address,address,uint256) (
    ↪ Launchpad_Core-main/KommunitasFactory.sol#773-786):
```

```
        - (success,data) = token.call(abi.encodeWithSelector(0xa9059cbb,
            ↪ to,value)) (Launchpad_Core-main/KommunitasFactory.sol
            ↪ #779-781)
Low level call in TransferHelper.safeTransferFrom(address,address,
    ↪ address,uint256) (Launchpad_Core-main/KommunitasFactory.sol
    ↪ #788-802):
        - (success,data) = token.call(abi.encodeWithSelector(0x23b872dd,
            ↪ from,to,value)) (Launchpad_Core-main/KommunitasFactory.sol
            ↪ #795-797)
Low level call in TransferHelper.safeTransferETH(address,uint256) (
    ↪ Launchpad_Core-main/KommunitasFactory.sol#804-807):
        - (success) = to.call{value: value}(new bytes(0)) (Launchpad_Core
            ↪ -main/KommunitasFactory.sol#805)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation
    ↪ #low-level-calls

Function IUniswapV2Pair.DOMAIN_SEPARATOR() (Launchpad_Core-main/
    ↪ KommunitasFactory.sol#877) is not in mixedCase
Function IUniswapV2Pair.PERMIT_TYPEHASH() (Launchpad_Core-main/
    ↪ KommunitasFactory.sol#879) is not in mixedCase
Function IUniswapV2Pair.MINIMUM_LIQUIDITY() (Launchpad_Core-main/
    ↪ KommunitasFactory.sol#910) is not in mixedCase
Parameter KommunitasProject.initialize(address,address,uint256,uint256,
    ↪ uint256,uint256,uint256,uint256[3],uint256[2],uint256,uint256,
    ↪ uint256)._payment (Launchpad_Core-main/KommunitasFactory.sol
    ↪ #1200) is not in mixedCase
Parameter KommunitasProject.initialize(address,address,uint256,uint256,
    ↪ uint256,uint256,uint256,uint256[3],uint256[2],uint256,uint256,
    ↪ uint256)._adminProject (Launchpad_Core-main/KommunitasFactory.sol
    ↪ #1201) is not in mixedCase
Parameter KommunitasProject.initialize(address,address,uint256,uint256,
    ↪ uint256,uint256,uint256,uint256[3],uint256[2],uint256,uint256,
    ↪ uint256)._tokenProjectDecimals (Launchpad_Core-main/
    ↪ KommunitasFactory.sol#1202) is not in mixedCase
```

```
Parameter KommunitasProject.initialize(address,address,uint256,uint256,
    ↪ uint256,uint256,uint256,uint256[3],uint256[2],uint256,uint256,
    ↪ uint256)._sale (Launchpad_Core-main/KommunitasFactory.sol#1203)
    ↪ is not in mixedCase
Parameter KommunitasProject.initialize(address,address,uint256,uint256,
    ↪ uint256,uint256,uint256,uint256[3],uint256[2],uint256,uint256,
    ↪ uint256)._target (Launchpad_Core-main/KommunitasFactory.sol#1204)
    ↪  is not in mixedCase
Parameter KommunitasProject.initialize(address,address,uint256,uint256,
    ↪ uint256,uint256,uint256,uint256[3],uint256[2],uint256,uint256,
    ↪ uint256)._calculation (Launchpad_Core-main/KommunitasFactory.sol
    ↪ #1205) is not in mixedCase
Parameter KommunitasProject.initialize(address,address,uint256,uint256,
    ↪ uint256,uint256,uint256,uint256[3],uint256[2],uint256,uint256,
    ↪ uint256)._start (Launchpad_Core-main/KommunitasFactory.sol#1206)
    ↪ is not in mixedCase
Parameter KommunitasProject.initialize(address,address,uint256,uint256,
    ↪ uint256,uint256,uint256,uint256[3],uint256[2],uint256,uint256,
    ↪ uint256)._price (Launchpad_Core-main/KommunitasFactory.sol#1207)
    ↪ is not in mixedCase
Parameter KommunitasProject.initialize(address,address,uint256,uint256,
    ↪ uint256,uint256,uint256,uint256[3],uint256[2],uint256,uint256,
    ↪ uint256)._minMaxPublicBuy (Launchpad_Core-main/KommunitasFactory.
    ↪ sol#1208) is not in mixedCase
Parameter KommunitasProject.initialize(address,address,uint256,uint256,
    ↪ uint256,uint256,uint256,uint256[3],uint256[2],uint256,uint256,
    ↪ uint256)._tge (Launchpad_Core-main/KommunitasFactory.sol#1209) is
    ↪  not in mixedCase
Parameter KommunitasProject.initialize(address,address,uint256,uint256,
    ↪ uint256,uint256,uint256,uint256[3],uint256[2],uint256,uint256,
    ↪ uint256)._boosterRunning (Launchpad_Core-main/KommunitasFactory.
    ↪ sol#1210) is not in mixedCase
Parameter KommunitasProject.initialize(address,address,uint256,uint256,
    ↪ uint256,uint256,uint256,uint256[3],uint256[2],uint256,uint256,
```

```
    ↪ uint256)._boosterDelay (Launchpad_Core-main/KommunitasFactory.sol
    ↪ #1211) is not in mixedCase
Parameter KommunitasProject.getBuyerHistoryLength(address)._buyer (
    ↪ Launchpad_Core-main/KommunitasFactory.sol#1270) is not in
    ↪ mixedCase
Parameter KommunitasProject.getUserStakedInfo(KommunitasProject.
    ↪ StakingChoice,address)._choice (Launchpad_Core-main/
    ↪ KommunitasFactory.sol#1298) is not in mixedCase
Parameter KommunitasProject.getUserStakedInfo(KommunitasProject.
    ↪ StakingChoice,address)._target (Launchpad_Core-main/
    ↪ KommunitasFactory.sol#1298) is not in mixedCase
Function KommunitasProject.getUserAllocation_d8(address) (Launchpad_Core
    ↪ -main/KommunitasFactory.sol#1328-1344) is not in mixedCase
Parameter KommunitasProject.getUserAllocation_d8(address)._target (
    ↪ Launchpad_Core-main/KommunitasFactory.sol#1328) is not in
    ↪ mixedCase
Parameter KommunitasProject.isBuyer(address)._user (Launchpad_Core-main/
    ↪ KommunitasFactory.sol#1350) is not in mixedCase
Parameter KommunitasProject.getAmountOut(address,uint256)._tokenIn (
    ↪ Launchpad_Core-main/KommunitasFactory.sol#1360) is not in
    ↪ mixedCase
Parameter KommunitasProject.getAmountOut(address,uint256)._amountIn (
    ↪ Launchpad_Core-main/KommunitasFactory.sol#1360) is not in
    ↪ mixedCase
Parameter KommunitasProject.getTotalPurchase(address)._user (
    ↪ Launchpad_Core-main/KommunitasFactory.sol#1379) is not in
    ↪ mixedCase
Parameter KommunitasProject.getUserAllocToken(address)._user (
    ↪ Launchpad_Core-main/KommunitasFactory.sol#1430) is not in
    ↪ mixedCase
Parameter KommunitasProject.amountInCalc(uint256,uint256,address).
    ↪ _tokenReceived (Launchpad_Core-main/KommunitasFactory.sol#1464)
    ↪ is not in mixedCase
```

```
Parameter KommunitasProject.amountInCalc(uint256,uint256,address).
    ↪ _amountIn (Launchpad_Core-main/KommunitasFactory.sol#1465) is not
    ↪  in mixedCase
Parameter KommunitasProject.amountInCalc(uint256,uint256,address)._user
    ↪ (Launchpad_Core-main/KommunitasFactory.sol#1466) is not in
    ↪ mixedCase
Parameter KommunitasProject.amountInCalcInner(address,uint256,uint256).
    ↪ _user (Launchpad_Core-main/KommunitasFactory.sol#1509) is not in
    ↪ mixedCase
Parameter KommunitasProject.amountInCalcInner(address,uint256,uint256).
    ↪ _tokenReceived (Launchpad_Core-main/KommunitasFactory.sol#1510)
    ↪ is not in mixedCase
Parameter KommunitasProject.amountInCalcInner(address,uint256,uint256).
    ↪ _amountIn (Launchpad_Core-main/KommunitasFactory.sol#1511) is not
    ↪  in mixedCase
Parameter KommunitasProject.buyTokenByETH(address[])._path (
    ↪ Launchpad_Core-main/KommunitasFactory.sol#1598) is not in
    ↪ mixedCase
Parameter KommunitasProject.buyTokenByToken(uint256,address[])._amountIn
    ↪  (Launchpad_Core-main/KommunitasFactory.sol#1669) is not in
    ↪ mixedCase
Parameter KommunitasProject.buyTokenByToken(uint256,address[])._path (
    ↪ Launchpad_Core-main/KommunitasFactory.sol#1669) is not in
    ↪ mixedCase
Parameter KommunitasProject.buyToken(uint256,address)._amountIn (
    ↪ Launchpad_Core-main/KommunitasFactory.sol#1738) is not in
    ↪ mixedCase
Parameter KommunitasProject.buyToken(uint256,address)._tokenIn (
    ↪ Launchpad_Core-main/KommunitasFactory.sol#1738) is not in
    ↪ mixedCase
Parameter KommunitasProject.setBuyer(address)._user (Launchpad_Core-main
    ↪ /KommunitasFactory.sol#1802) is not in mixedCase
Parameter KommunitasProject.setRecipient(string)._recipient (
    ↪ Launchpad_Core-main/KommunitasFactory.sol#1820) is not in
```

```
    ↪ mixedCase
Parameter KommunitasProject.swapToAccepted(uint256,address[],address).
    ↪ _amountIn (Launchpad_Core-main/KommunitasFactory.sol#1831) is not
    ↪  in mixedCase
Parameter KommunitasProject.swapToAccepted(uint256,address[],address).
    ↪ _path (Launchpad_Core-main/KommunitasFactory.sol#1832) is not in
    ↪ mixedCase
Parameter KommunitasProject.swapToAccepted(uint256,address[],address).
    ↪ _to (Launchpad_Core-main/KommunitasFactory.sol#1833) is not in
    ↪ mixedCase
Function KommunitasProject.setWhitelist_d6(address[],uint256[]) (
    ↪ Launchpad_Core-main/KommunitasFactory.sol#1953-1969) is not in
    ↪ mixedCase
Parameter KommunitasProject.setWhitelist_d6(address[],uint256[])._user (
    ↪ Launchpad_Core-main/KommunitasFactory.sol#1954) is not in
    ↪ mixedCase
Parameter KommunitasProject.setWhitelist_d6(address[],uint256[]).
    ↪ _allocation (Launchpad_Core-main/KommunitasFactory.sol#1955) is
    ↪ not in mixedCase
Parameter KommunitasProject.setTge(uint256)._tge (Launchpad_Core-main/
    ↪ KommunitasFactory.sol#1974) is not in mixedCase
Parameter KommunitasProject.transferOwnership(address)._newOwner (
    ↪ Launchpad_Core-main/KommunitasFactory.sol#1992) is not in
    ↪ mixedCase
Parameter KommunitasFactory.createProject(address,address,uint256,
    ↪ uint256,uint256,uint256,uint256,uint256[3],uint256[2],uint256,
    ↪ uint256,uint256)._payment (Launchpad_Core-main/KommunitasFactory.
    ↪ sol#2074) is not in mixedCase
Parameter KommunitasFactory.createProject(address,address,uint256,
    ↪ uint256,uint256,uint256,uint256,uint256[3],uint256[2],uint256,
    ↪ uint256,uint256)._adminProject (Launchpad_Core-main/
    ↪ KommunitasFactory.sol#2075) is not in mixedCase
Parameter KommunitasFactory.createProject(address,address,uint256,
    ↪ uint256,uint256,uint256,uint256,uint256[3],uint256[2],uint256,
```

```
    ↪ uint256,uint256)._tokenProjectDecimals (Launchpad_Core-main/
    ↪ KommunitasFactory.sol#2076) is not in mixedCase
Parameter KommunitasFactory.createProject(address,address,uint256,
    ↪ uint256,uint256,uint256,uint256,uint256[3],uint256[2],uint256,
    ↪ uint256,uint256)._sale (Launchpad_Core-main/KommunitasFactory.sol
    ↪ #2077) is not in mixedCase
Parameter KommunitasFactory.createProject(address,address,uint256,
    ↪ uint256,uint256,uint256,uint256,uint256[3],uint256[2],uint256,
    ↪ uint256,uint256)._target (Launchpad_Core-main/KommunitasFactory.
    ↪ sol#2078) is not in mixedCase
Parameter KommunitasFactory.createProject(address,address,uint256,
    ↪ uint256,uint256,uint256,uint256,uint256[3],uint256[2],uint256,
    ↪ uint256,uint256)._calculation (Launchpad_Core-main/
    ↪ KommunitasFactory.sol#2079) is not in mixedCase
Parameter KommunitasFactory.createProject(address,address,uint256,
    ↪ uint256,uint256,uint256,uint256,uint256[3],uint256[2],uint256,
    ↪ uint256,uint256)._start (Launchpad_Core-main/KommunitasFactory.
    ↪ sol#2080) is not in mixedCase
Parameter KommunitasFactory.createProject(address,address,uint256,
    ↪ uint256,uint256,uint256,uint256,uint256[3],uint256[2],uint256,
    ↪ uint256,uint256)._price (Launchpad_Core-main/KommunitasFactory.
    ↪ sol#2081) is not in mixedCase
Parameter KommunitasFactory.createProject(address,address,uint256,
    ↪ uint256,uint256,uint256,uint256,uint256[3],uint256[2],uint256,
    ↪ uint256,uint256)._minMaxPublicBuy (Launchpad_Core-main/
    ↪ KommunitasFactory.sol#2082) is not in mixedCase
Parameter KommunitasFactory.createProject(address,address,uint256,
    ↪ uint256,uint256,uint256,uint256,uint256[3],uint256[2],uint256,
    ↪ uint256,uint256)._tge (Launchpad_Core-main/KommunitasFactory.sol
    ↪ #2083) is not in mixedCase
Parameter KommunitasFactory.createProject(address,address,uint256,
    ↪ uint256,uint256,uint256,uint256,uint256[3],uint256[2],uint256,
    ↪ uint256,uint256)._boosterRunning (Launchpad_Core-main/
    ↪ KommunitasFactory.sol#2084) is not in mixedCase
```

```
Parameter KommunitasFactory.createProject(address,address,uint256,
    ↪ uint256,uint256,uint256,uint256,uint256[3],uint256[2],uint256,
    ↪ uint256,uint256)._boosterDelay (Launchpad_Core-main/
    ↪ KommunitasFactory.sol#2085) is not in mixedCase
Parameter KommunitasFactory.transferOwnership(address)._newOwner (
    ↪ Launchpad_Core-main/KommunitasFactory.sol#2128) is not in
    ↪ mixedCase
Parameter KommunitasFactory.setSwapFactory(address)._swapFactory (
    ↪ Launchpad_Core-main/KommunitasFactory.sol#2137) is not in
    ↪ mixedCase
Parameter KommunitasFactory.setPayment(address)._token (Launchpad_Core-
    ↪ main/KommunitasFactory.sol#2146) is not in mixedCase
Parameter KommunitasFactory.removePayment(address)._token (
    ↪ Launchpad_Core-main/KommunitasFactory.sol#2163) is not in
    ↪ mixedCase
Parameter KommunitasFactory.setDevAddr(address)._devAddr (Launchpad_Core
    ↪ -main/KommunitasFactory.sol#2184) is not in mixedCase
Parameter KommunitasFactory.getPaymentIndex(address)._token (
    ↪ Launchpad_Core-main/KommunitasFactory.sol#2193) is not in
    ↪ mixedCase
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation
    ↪ #conformance-to-solidity-naming-conventions

Redundant expression "this (Launchpad_Core-main/KommunitasFactory.sol
    ↪ #21)" inContext (Launchpad_Core-main/KommunitasFactory.sol#15-24)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation
    ↪ #redundant-statements

Variable KommunitasProject.getUserAllocation_d8(address).userV1Staked (
    ↪ Launchpad_Core-main/KommunitasFactory.sol#1333) is too similar to
    ↪  KommunitasProject.getUserAllocation_d8(address).userV2Staked (
    ↪ Launchpad_Core-main/KommunitasFactory.sol#1337)
Variable KommunitasProject.getUserAllocation_d8(address).v1TotalStaked (
    ↪ Launchpad_Core-main/KommunitasFactory.sol#1333) is too similar to
```

```
    ↪  KommunitasProject.getUserAllocation_d8(address).v2TotalStaked (
    ↪ Launchpad_Core-main/KommunitasFactory.sol#1337)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation
    ↪ #variable-names-are-too-similar

name() should be declared external:
        - ERC20.name() (Launchpad_Core-main/KommunitasFactory.sol
            ↪ #342-344)
symbol() should be declared external:
        - ERC20.symbol() (Launchpad_Core-main/KommunitasFactory.sol
            ↪ #350-352)
decimals() should be declared external:
        - ERC20.decimals() (Launchpad_Core-main/KommunitasFactory.sol
            ↪ #367-369)
totalSupply() should be declared external:
        - ERC20.totalSupply() (Launchpad_Core-main/KommunitasFactory.sol
            ↪ #374-376)
balanceOf(address) should be declared external:
        - ERC20.balanceOf(address) (Launchpad_Core-main/KommunitasFactory
            ↪ .sol#381-383)
transfer(address,uint256) should be declared external:
        - ERC20.transfer(address,uint256) (Launchpad_Core-main/
            ↪ KommunitasFactory.sol#393-401)
allowance(address,address) should be declared external:
        - ERC20.allowance(address,address) (Launchpad_Core-main/
            ↪ KommunitasFactory.sol#406-414)
approve(address,uint256) should be declared external:
        - ERC20.approve(address,uint256) (Launchpad_Core-main/
            ↪ KommunitasFactory.sol#423-431)
transferFrom(address,address,uint256) should be declared external:
        - ERC20.transferFrom(address,address,uint256) (Launchpad_Core-
            ↪ main/KommunitasFactory.sol#446-461)
increaseAllowance(address,uint256) should be declared external:
```

```
        - ERC20.increaseAllowance(address,uint256) (Launchpad_Core-main/
            ↪ KommunitasFactory.sol#475-486)
decreaseAllowance(address,uint256) should be declared external:
        - ERC20.decreaseAllowance(address,uint256) (Launchpad_Core-main/
            ↪ KommunitasFactory.sol#502-516)
initialize(address,address,uint256,uint256,uint256,uint256,uint256,
    ↪ uint256[3],uint256[2],uint256,uint256,uint256) should be declared
    ↪  external:
        - KommunitasProject.initialize(address,address,uint256,uint256,
            ↪ uint256,uint256,uint256,uint256[3],uint256[2],uint256,
            ↪ uint256,uint256) (Launchpad_Core-main/KommunitasFactory.
            ↪ sol#1199-1249)
getWhitelistLength() should be declared external:
        - KommunitasProject.getWhitelistLength() (Launchpad_Core-main/
            ↪ KommunitasFactory.sol#1256-1258)
getBuyersLength() should be declared external:
        - KommunitasProject.getBuyersLength() (Launchpad_Core-main/
            ↪ KommunitasFactory.sol#1263-1265)
getBuyerHistoryLength(address) should be declared external:
        - KommunitasProject.getBuyerHistoryLength(address) (
            ↪ Launchpad_Core-main/KommunitasFactory.sol#1270-1276)
getTotalPurchase(address) should be declared external:
        - KommunitasProject.getTotalPurchase(address) (Launchpad_Core-
            ↪ main/KommunitasFactory.sol#1379-1387)
moveFund() should be declared external:
        - KommunitasProject.moveFund() (Launchpad_Core-main/
            ↪ KommunitasFactory.sol#1583-1592)
buyTokenByETH(address[]) should be declared external:
        - KommunitasProject.buyTokenByETH(address[]) (Launchpad_Core-main
            ↪ /KommunitasFactory.sol#1598-1662)
buyTokenByToken(uint256,address[]) should be declared external:
        - KommunitasProject.buyTokenByToken(uint256,address[]) (
            ↪ Launchpad_Core-main/KommunitasFactory.sol#1669-1731)
buyToken(uint256,address) should be declared external:
```

```
        - KommunitasProject.buyToken(uint256,address) (Launchpad_Core-
            ↪ main/KommunitasFactory.sol#1738-1796)
setRecipient(string) should be declared external:
        - KommunitasProject.setRecipient(string) (Launchpad_Core-main/
            ↪ KommunitasFactory.sol#1820-1822)
setWhitelist_d6(address[],uint256[]) should be declared external:
        - KommunitasProject.setWhitelist_d6(address[],uint256[]) (
            ↪ Launchpad_Core-main/KommunitasFactory.sol#1953-1969)
setTge(uint256) should be declared external:
        - KommunitasProject.setTge(uint256) (Launchpad_Core-main/
            ↪ KommunitasFactory.sol#1974-1977)
setV2Staked() should be declared external:
        - KommunitasProject.setV2Staked() (Launchpad_Core-main/
            ↪ KommunitasFactory.sol#1982-1990)
transferOwnership(address) should be declared external:
        - KommunitasProject.transferOwnership(address) (Launchpad_Core-
            ↪ main/KommunitasFactory.sol#1992-1995)
togglePause() should be declared external:
        - KommunitasProject.togglePause() (Launchpad_Core-main/
            ↪ KommunitasFactory.sol#1997-1999)
allProjectsLength() should be declared external:
        - KommunitasFactory.allProjectsLength() (Launchpad_Core-main/
            ↪ KommunitasFactory.sol#2047-2049)
allPaymentsLength() should be declared external:
        - KommunitasFactory.allPaymentsLength() (Launchpad_Core-main/
            ↪ KommunitasFactory.sol#2054-2056)
createProject(address,address,uint256,uint256,uint256,uint256,uint256,
    ↪ uint256[3],uint256[2],uint256,uint256,uint256) should be declared
    ↪  external:
        - KommunitasFactory.createProject(address,address,uint256,uint256
            ↪ ,uint256,uint256,uint256,uint256[3],uint256[2],uint256,
            ↪ uint256,uint256) (Launchpad_Core-main/KommunitasFactory.
            ↪ sol#2073-2122)
transferOwnership(address) should be declared external:
```

```
        - KommunitasFactory.transferOwnership(address) (Launchpad_Core-
            ↪ main/KommunitasFactory.sol#2128-2131)
setSwapFactory(address) should be declared external:
        - KommunitasFactory.setSwapFactory(address) (Launchpad_Core-main/
            ↪ KommunitasFactory.sol#2137-2140)
setPayment(address) should be declared external:
        - KommunitasFactory.setPayment(address) (Launchpad_Core-main/
            ↪ KommunitasFactory.sol#2146-2157)
removePayment(address) should be declared external:
        - KommunitasFactory.removePayment(address) (Launchpad_Core-main/
            ↪ KommunitasFactory.sol#2163-2178)
setDevAddr(address) should be declared external:
        - KommunitasFactory.setDevAddr(address) (Launchpad_Core-main/
            ↪ KommunitasFactory.sol#2184-2187)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation
    ↪ #public-function-that-could-be-declared-external
Launchpad_Core-main/KommunitasFactory.sol analyzed (14 contracts with 78
    ↪  detectors), 152 result(s) found
```

Conclusion:

Most of the vulnerabilities found by the analysis have already been addressed by the smart contract code review.

5 Conclusion

In this audit, we examined the design and implementation of Kommunitas contract and discovered several issues of varying severity. Kommunitas team addressed 4 issues raised in the initial report and implemented the necessary fixes, while classifying the rest as a risk with low-probability of occurrence. Shellboxes' auditors advised Kommunitas Team to maintain a high level of vigilance and to keep those findings in mind in order to avoid any future complications.

For a Contract Audit, contact us at contact@shellboxes.com