METATRUST

Draft
Security Assessment for

Hack-20210603-PancakeHunny (1OK-FLP)

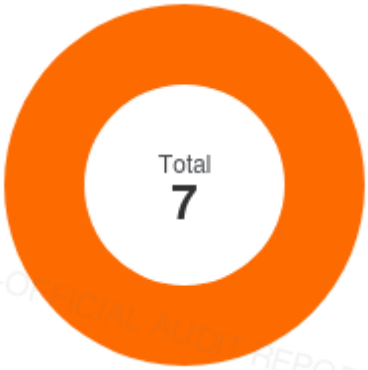
July 23, 2023

Executive Summary

Overview	
Project Name	Hack-20210603-PancakeHunny (1OK-FLP)
Codebase URL	-
Scan Engine	AI Analyzer
Scan Time	2023/07/23 15:15:49
Commit Id	-

Total	
Critical Issues	0
High risk Issues	7
Medium risk Issues	0
Low risk Issues	0
Informational Issues	0

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



Critical Issues	0%	0
High risk Issues	100%	7
Medium risk Issues	0%	0
Low risk Issues	0%	0
Informational Issues	0%	0

Summary of Findings

MetaScan security assessment was performed on **July 23, 2023 15:15:49** on project **Hack-20210603-PancakeHunny (1OK-FLP)** with the repository **Hack_20210603_PancakeHunny** on branch **default branch**. The assessment was carried out by scanning the project's codebase using the scan engine **AI Analyzer**. There are in total **7** vulnerabilities / security risks discovered during the scanning session, among which **0** critical vulnerabilities, **7** high risk vulnerabilities, **0** medium risk vulnerabilities, **0** low risk vulnerabilities, **0** informational issues.

ID	Description	Severity
MSA-001	MWE-200: Insecure LP Token Value Calculation	High risk
MSA-002	MWE-200: Insecure LP Token Value Calculation	High risk
MSA-003	MWE-200: Insecure LP Token Value Calculation	High risk
MSA-004	MWE-200: Insecure LP Token Value Calculation	High risk
MSA-005	MWE-200: Insecure LP Token Value Calculation	High risk
MSA-006	MWE-200: Insecure LP Token Value Calculation	High risk
MSA-007	MWE-200: Insecure LP Token Value Calculation	High risk

NON-OFFICIAL AUDIT REPORT

Findings

Critical (0)

No Critical vulnerabilities found here

High risk (7)

1. MWE-200: Insecure LP Token Value Calculation

High risk Security Analyzer

Liquidity token value/price can be manipulated to cause flashloan attacks.

File(s) Affected

HunnyMinter.sol #1882-1886

```
1882    function getReserves(address factory, address tokenA, address tokenB) internal view returns (uint
1883        (address token0,) = sortTokens(tokenA, tokenB);
1884        (uint reserve0, uint reserve1,) = IUniswapV2Pair(pairFor(factory, tokenA, tokenB)).getReserve
1885        (reserveA, reserveB) = tokenA == token0 ? (reserve0, reserve1) : (reserve1, reserve0);
1886    }
```

HunnyMinter.sol #3191-3203

```
3191    function unsafeTokenPriceInBNB(address _token) private view returns(uint) {
3192        address pair = factory.getPair(_token, address(WBNB));
3193        uint decimal = uint(BEP20(_token).decimals());
3194
3195        (uint reserve0, uint reserve1, ) = IPancakePair(pair).getReserves();
3196        if (IPancakePair(pair).token0() == _token) {
3197            return reserve1.mul(10**decimal).div(reserve0);
3198        } else if (IPancakePair(pair).token1() == _token) {
3199            return reserve0.mul(10**decimal).div(reserve1);
3200        } else {
3201            return 0;
3202        }
3203    }
```

Recommendation

Do not use AMM pool or custom liquidity calculation to caculate LP token value/price.

2. MWE-200: Insecure LP Token Value Calculation

High risk Security Analyzer

Liquidity token value/price can be manipulated to cause flashloan attacks.

File(s) Affected

HunnyMinter.sol #2715-2729

```
2715    function generateFlipToken() private returns(uint liquidity) {
2716        uint amountADesired = IBEP20(_hunny).balanceOf(address(this));
2717        uint amountBDesired = IBEP20(_wbnb).balanceOf(address(this));
2718
2719        IBEP20(_hunny).safeApprove(address(ROUTER), 0);
2720        IBEP20(_hunny).safeApprove(address(ROUTER), amountADesired);
2721        IBEP20(_wbnb).safeApprove(address(ROUTER), 0);
2722        IBEP20(_wbnb).safeApprove(address(ROUTER), amountBDesired);
2723
2724        (,,liquidity) = ROUTER.addLiquidity(_hunny, _wbnb, amountADesired, amountBDesired, 0, 0, addr
2725
2726        // send dust
2727        IBEP20(_hunny).transfer(msg.sender, IBEP20(_hunny).balanceOf(address(this)));
2728        IBEP20(_wbnb).transfer(msg.sender, IBEP20(_wbnb).balanceOf(address(this)));
2729    }
```

Recommendation

Do not use AMM pool or custom liquidity calculation to caculate LP token value/price.

NON-OFFICIAL AUDIT REPORT

3. MWE-200: Insecure LP Token Value Calculation

High risk Security Analyzer

Liquidity token value/price can be manipulated to cause flashloan attacks.

File(s) Affected

HunnyMinter.sol #3243-3247

```
3243    function _apy(uint pid) view private returns(uint) {
3244        (address token,,,) = master.poolInfo(pid);
3245        uint poolSize = tvl(token, IBEP20(token).balanceOf(address(master))).mul(1e18).div(bnbPriceIn
3246        return cakePriceInBNB().mul(cakePerYearOfPool(pid)).div(poolSize);
3247    }
```

HunnyMinter.sol #3305-3316

```
3305    function compoundingAPY(uint pid, uint compoundUnit) view public returns(uint) {
3306        uint __apy = _apy(pid);
3307        uint compoundTimes = 365 days / compoundUnit;
3308        uint unitAPY = 1e18 + (__apy / compoundTimes);
3309        uint result = 1e18;
3310
3311        for(uint i=0; i<compoundTimes; i++) {
3312            result = (result * unitAPY) / 1e18;
3313        }
3314
3315        return result - 1e18;
3316    }
```

Recommendation

Do not use AMM pool or custom liquidity calculation to caculate LP token value/price.

NON-OFFICIAL AUDIT REPORT

4. MWE-200: Insecure LP Token Value Calculation

High risk Security Analyzer

Liquidity token value/price can be manipulated to cause flashloan attacks.

File(s) Affected

HunnyMinter.sol #3255-3279

```
3255    function tvl(address _flip, uint amount) public view returns (uint) {
3256        if (_flip == address(CAKE)) {
3257            return cakePriceInBNB().mul(bnbPriceInUSD()).mul(amount).div(1e36);
3258        }
3259        address _token0 = IPancakePair(_flip).token0();
3260        address _token1 = IPancakePair(_flip).token1();
3261
3262        // using hunny price from the oracle
3263        if (_token0 == address(hunny) || _token1 == address(hunny)) {
3264            uint hunnyBalance = hunny.balanceOf(address(_flip)).mul(amount).div(IBEP20(_flip).totalSu
3265            uint priceInBNB = tokenPriceInBNB(address(hunny));
3266            uint price = priceInBNB.mul(bnbPriceInUSD()).div(1e18);
3267            return hunnyBalance.mul(price).div(1e18).mul(2);
3268        }
3269
3270        if (_token0 == address(WBNB) || _token1 == address(WBNB)) {
3271            uint bnb = WBNB.balanceOf(address(_flip)).mul(amount).div(IBEP20(_flip).totalSupply());
3272            uint price = bnbPriceInUSD();
3273            return bnb.mul(price).div(1e18).mul(2);
3274        }
3275
3276        uint balanceToken0 = IBEP20(_token0).balanceOf(_flip);
3277        uint price = tokenPriceInBNB(_token0);
3278        return balanceToken0.mul(price).div(1e18).mul(bnbPriceInUSD()).div(1e18).mul(2);
3279    }
```

Recommendation

Do not use AMM pool or custom liquidity calculation to caculate LP token value/price.

5. MWE-200: Insecure LP Token Value Calculation

High risk Security Analyzer

Liquidity token value/price can be manipulated to cause flashloan attacks.

File(s) Affected

HunnyMinter.sol #3281-3303

```
3281      function tvlInBNB(address _flip, uint amount) public view returns (uint) {
3282          if (_flip == address(CAKE)) {
3283              return cakePriceInBNB().mul(amount).div(1e18);
3284          }
3285          address _token0 = IPancakePair(_flip).token0();
3286          address _token1 = IPancakePair(_flip).token1();
3287
3288          // using hunny price from the oracle
3289          if (_token0 == address(hunny) || _token1 == address(hunny)) {
3290              uint hunnyBalance = hunny.balanceOf(address(_flip)).mul(amount).div(IBEP20(_flip).totalSu
3291              uint priceInBNB = tokenPriceInBNB(address(hunny));
3292              return hunnyBalance.mul(priceInBNB).div(1e18).mul(2);
3293          }
3294
3295          if (_token0 == address(WBNB) || _token1 == address(WBNB)) {
3296              uint bnb = WBNB.balanceOf(address(_flip)).mul(amount).div(IBEP20(_flip).totalSupply());
3297              return bnb.mul(2);
3298          }
3299
3300          uint balanceToken0 = IBEP20(_token0).balanceOf(_flip);
3301          uint price = tokenPriceInBNB(_token0);
3302          return balanceToken0.mul(price).div(1e18).mul(2);
3303      }
```

Recommendation

Do not use AMM pool or custom liquidity calculation to caculate LP token value/price.

NON-OFFICIAL AUDIT REPORT

6. MWE-200: Insecure LP Token Value Calculation

High risk Security Analyzer

Liquidity token value/price can be manipulated to cause flashloan attacks.

File(s) Affected

HunnyMinter.sol #3763-3777

```
3763     function apy() override public view returns(uint _usd, uint _hunny, uint _bnb) {
3764         uint tokenDecimals = 1e18;
3765         uint __totalSupply = _totalSupply;
3766         if (__totalSupply == 0) {
3767             __totalSupply = tokenDecimals;
3768         }
3769
3770         uint rewardPerTokenPerSecond = rewardRate.mul(tokenDecimals).div(__totalSupply);
3771         uint hunnyPrice = helper.tokenPriceInBNB(address(stakingToken));
3772         uint flipPrice = helper.tvlInBNB(address(rewardsToken), 1e18);
3773
3774         _usd = 0;
3775         _hunny = 0;
3776         _bnb = rewardPerTokenPerSecond.mul(365 days).mul(flipPrice).div(hunnyPrice);
3777     }
```

Recommendation

Do not use AMM pool or custom liquidity calculation to caculate LP token value/price.

7. MWE-200: Insecure LP Token Value Calculation

High risk | Security Analyzer

Liquidity token value/price can be manipulated to cause flashloan attacks.

File(s) Affected

HunnyMinter.sol #4523-4531

```
4523    function tvl() override public view returns (uint) {
4524        uint stakingTVL = helper.tvl(address(stakingToken), _totalSupply);
4525
4526        uint price = rewardsToken.priceShare();
4527        uint earned = rewardsToken.balanceOf(address(this)).mul(price).div(1e18);
4528        uint rewardTVL = helper.tvl(CAKE, earned);
4529
4530        return stakingTVL.add(rewardTVL);
4531    }
```

HunnyMinter.sol #3229-3240

```
3229    function profitOf(address minter, address flip, uint amount) external view returns (uint _usd, ui
3230        _usd = tvl(flip, amount);
3231        if (address(minter) == address(0)) {
3232            _hunny = 0;
3233        } else {
3234            uint performanceFee = IHunnyMinter(minter).performanceFee(_usd);
3235            _usd = _usd.sub(performanceFee);
3236            uint bnbAmount = performanceFee.mul(1e18).div(bnbPriceInUSD());
3237            _hunny = IHunnyMinter(minter).amountHunnyToMint(bnbAmount);
3238        }
3239        _bnb = 0;
3240    }
```

Recommendation

Do not use AMM pool or custom liquidity calculation to caculate LP token value/price.

Medium risk (0)

No Medium risk vulnerabilities found here

Low risk (0)

No Low risk vulnerabilities found here

Informational (0)

No Informational vulnerabilities found here

Disclaimer

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

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

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

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

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

ALL SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF ARE PROVIDED "AS IS" AND "AS Hack-20210603-PancakeHunny (1OK-FLP) Security Assessment AVAILABLE" AND WITH ALL FAULTS AND DEFECTS WITHOUT WARRANTY OF ANY KIND. TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW,

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

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

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

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

NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING Hack-20210603-PancakeHunny (1OK-FLP) Security Assessment MATERIALS AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST MetaTrust WITH RESPECT TO SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING MATERIALS.

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

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