Recklessness Comes at a Cost? Zunami Protocol Attacked for Price Manipulation with a Loss of \$2.1M



On August 14, 2023, Beosin EagleEye detected a price manipulation attack on the Zunami Protocol, a protocol on the Ethereum blockchain. The attack resulted in a loss of 1152 ETH(\$2.1 million).

It is understood that the Zunami Protocol is a platform that distributes stablecoins to users. It can be seen as a decentralized yield aggregator, providing more beneficial solutions for stablecoin holders.

There is an interesting twist to this incident. A security company had previously warned about vulnerabilities, but the project team did not take these warnings seriously, displaying a nonchalant attitude. As a consequence, by the time the incident occurred, it was already too late.

Beosin security team promptly analyzed the security incident and reported the following findings:

Attack-related Information:

• Attack Transactions:

Ί.	\v_1	

0x2aec4fdb2a09ad4269a410f2c770737626fb62c54e0fa8ac25e8582d4b690cca

Tx2:

0x0788ba222970c7c68a738b0e08fb197e669e61f9b226ceec4cab9b85abe8cceb

• Attacker's Address:

0x5f4c21c9bb73c8b4a296cc256cocde324db146df

• Attack Contract:

0xa21a2b59d8odc42d332f778cbb9ea127100e5d75

• Targeted Contract:

0xe47f1cd2a37c6fe69e3501ae45eca263c5a87b2b

Vulnerability Analysis:

The cause of this attack was the vulnerability in the contract where LP (Liquidity Provider) price calculation depended on the contract's own CRV balance and the exchange ratio of CRV in the wETH/CRV pool. The attacker manipulated the LP price by injecting CRV into the contract and manipulating the exchange ratio of the wETH/CRV pool.

Attack Process:

Taking transaction 0x2aec4... as an example:

Attack Preparation:

1. The hacker borrowed 6811 ETH using a balancer: Vault flash loan as attack funds.

2. They exchanged 300 ETH borrowed through a flash loan for 84 zETH, preparing for the subsequent increase in zETH value

Attack Phase:

1. They exchanged 11 ETH for 35293 CRV and transferred it to the sEthFraxEthCurveConvex contract, enabling the attacker to manipulate the CRV balance in the sEthFraxEthCurveConvex contract for later manipulation.

```
| Coli |
```

2. They repeatedly exchanged 406 ETH for CRV in the wETH/CRV pool, causing the price of CRV to increase by approximately 10 times.

```
0x4eBdF703948ddCEA3B11f675B4D1Fba942414A14.vxchamge(hrcC=1,
neg(=false, neg(=0xA21a285Fd80dC42D332F779Cbb9eA127100e6d75) \rightarrow ()
                                                                                                                                                                                                                                                                         ATE2=406249999999999999999
[call]
                                                          0x4eBdFT03948ddCEA3B11f6T6B4D1Fba942414A14.exthange(arg0=1, arg1=2, 0x4eBdFT03948ddCEA3B11f6T5B4D1Fba942414A14.exthange(arg0=1, arg1=2,
                                                                                                                                                                                                                                                                           01:0740624999999999999990,
01:0740624999999999999990,
                                                                                                                                                                                                                                                                                                                                                                                                                                    urgl=0xA21x2869d80dC42D332F779Cb69eA127100e5d75) --
urgl=0xA21x2869d80dC42D332F779Cb69eA127100e5d75) --
[call]
                          DAYSHI [m]
                                                                                                                                                                                                                                                                                                                                                                                              meiefalre.
                                                                                                                                                                                                                                                                            nr=2*406249999999999999999999
                                                                                                                                                                                                                                                                                                                                                                                                                                    0x4eBdF703948ddCEA3B11f675B4D1Fba9dZ414A14.corthange(argC=1.
                                                          0x4eBdF703948ddCBA3B11f675B4D1Fba9d2414814.oxthang=(arg0=1. arg1=2.
                                                                                                                                                                                                                                                                            lealt] Didge
                                                                                                                                                                                                                                                                                                                                                                                              argi-false.
                                                         Ox4eBdF103948dd:EA3Bl1f675B4D1Fba942414A14.extbuge(arg0=1, arg1=2, 0x4eBdF103948dd:EA3Bl1f675B4D1Fba962414A14.extbuge(arg0=1, arg1=2,
                                                                                                                                                                                                                                                                           n::2=406249999999999999990,
n::2=40624999999999999990,
                                                                                                                                                                                                                                                                                                                                                                                                                                   arg(=0xA21a2869d80dC42D332F778Cb69eA127100e6d76) \rightarrow ()

arg(=0xA21a2869d80dC42D332F770Cb69eA127100e6d76) \rightarrow ()
[call][
[call]
                                    Si [m]
                                                                                                                                                                                                                                                                                                                                                                                              metefalre.
                                                        Ox4-B4F70394846CEA3B11f676B4D1Fba942414A14.enthangefarg0=1, arg1=2,
0x4-B4F70394846CEA3B11f675B4D1Fba942414A14.enthangefarg0=1, arg1=2,
                                                                                                                                                                                                                                                                          ###2*40624999999999999990, ###2*0.
                                                                                                                                                                                                                                                                                                                                                                                             m_1(i=false, m_2(i=0xA2)a2959d90dC42D93257780b59a4227100e5475) \rightarrow ()
m_2(i=false, m_2(i=0xA2)a2959d90dC42D93297780bb6e4127100e5d75) \rightarrow ()
 [call]
[call][
                           6000) [m]
                                                        Ox4+BdF7039484dCEA3Bl1f675B4D1Fb=942414A14.wxthunge(nrg)=1, nrg)=2,
0x4+BdF703948ddCEA3B11f675B4D1Fb=942414A14.wxthunge(nrg)=1, nrg)=2.
                                                                                                                                                                                                                                                                          11:0=406249999999999999990,
11:0=40624999999999999990,
                                                                                                                                                                                                                                                                                                                                                                                                                                  m_T(-0xA21a2B59d80dC42D3)25778Cbb9eA127100e6d75) \rightarrow ()

m_T(-0xA21a2B59d80dC42D3)25979Cbb9eA127100e5d75) \rightarrow ()
[call]
                                                                                                                                                                                                                                                                                                                                                                                              argarfalse.
                                                                                                                                                                                                                                                                                                                                                                  acc >0.
                                                                                                                                                                                                                                                                                                                                                                                              medefalre.
Icall1
                              8743 [m]
                          ###27-406249999999999999990, ####27-0,
                                                                                                                                                                                                                                                                                                                                                                                                                                   \underset{i:j:l=0}{\text{mig}} = 0 \times A21 \times 2859 \times d00 \times d420 \times 31277 \times 31271 \times 3
[call][1
                                                                                                                                                                                                                                                                                                                                                                                             orgiefales.
                                                                                                                                                                                                                                                                            httl=406249999999999999990,
                                      [[@] 0x4eBdF70394BddCEA3B11f676B4D1Fba9d2414A14.oxchunge(ung)-1, ing1-2,
                                                                                                                                                                                                                                                                                                                                                                                                                                    me_{T}(-0xA21a2859d00dC42D3328770Cbb9eA127100e5d75) \rightarrow ()
Icall11
[call][(108892][m] @x4+BdF70394840CEx3B116075B4D1Fba962414A14.wrchange(arg)=1, arg |=2.
                                                                                                                                                                                                                                                                                                                                                                                                                                    srg = 0xA21x2B59d80dC42D332F778Cbb9eA127100e5d75) \rightarrow ()
                                                                                                                                                                                                                                                                           htg2=40624999999999999990, htg2=0,
                                                                                                                                                                                                                                                                                                                                                                                             projectalos.
```

- 3. The value calculation of zETH (LP) depended on the price of CRV tokens and the valuation of CRV to ETH calculations in the sEthFraxEthCurveConvex contract.
- 4. The attacker manipulated the CRV price and the CRV balance in the vulnerable contract, causing the final _assetPriceCached to increase.

```
| (eall||(1000)|| (e) || (sEH)| containes Fried|| → () |
| Intuitive || (e) || (sEH)| containes Fried|| → () |
| (intuitive || (e) || (sEH)| containes Fried|| → () |
| (intuitive || (e) || (sEH)| containes Fried|| → () |
| (intuitive || (e) || (sEH)| containes Fried|| → () |
| (intuitive || (e) || (sEH)| containes Fried|| → () |
| (intuitive || (e) || (e) || (set || (e) || (e)
```

```
function cacheAssetPrice() public virtual {
    _blockCached = block.number;
    uint256 currentAssetPrice = assetPrice();

if (_assetPriceCached < currentAssetPrice) {
    _assetPriceCached = currentAssetPrice;
    emit CachedAssetPrice(_blockCached, _assetPriceCached);
}
</pre>
```

```
function assetPrice() public view override returns (uint256) {
return priceOracle.lpPrice();
}
```

```
function lpPrice() public view returns (uint256) {
 279
                    return calcTokenPrice(totalHoldings(), totalSupply());
 280
 281
262
             function totalHoldings() public view returns (uint256) {
263 ~
                  uint256 length = _poolInfo.length;
264
265
                  uint256 totalHold = 0;
                  for (uint256 pid = 0; pid < length; pid++) {
266 V
                       PoolInfo memory poolInfo = poolInfo[pid];
267
                       if (poolInfo .lpShares > 0 && poolInfo .enabled) {
268
269
                            totalHold += poolInfo .strategy.totalHoldings();
270
271
272
                  return totalHold;
273
274
unction totalHoldings() external view virtual returns (uint256) {
  uint256 crvLpHoldings = (cvxRewards.balanceOf(address(this)) * getCurvePoolPrice()) /
  CURVE_PRICE_DENOMINATOR;
  uint256 crvEarned = cvxRewards.earned(address(this)); 1.control crv balance
 uint256 amountIn = crvEarned + _config.crv.balanceOf(address(this));
  uint256 crvEarningsInFeeToken = rewardManager.valuate(
     address(_config.crv),
     amountIn
  uint256 cvxTotalCliffs = _config.cvx.totalCliffs();
  uint256 cvxRemainCliffs = cvxTotalCliffs -
  _config.cvx.totalSupply() /
  _config.cvx.reductionPerCliff();
  amountIn =
  (crvEarned * cvxRemainCliffs) /
  cvxTotalCliffs +
  config.cvx.balanceOf(address(this));
  uint256 cvxEarningsInFeeToken = rewardManager.valuate
     address(_config.cvx),
     amountIn
  );
  uint256 tokensHoldings = 0;
  for (uint256 i = 0; i < 3; i++) {
     tokensHoldings += balanceOfNative(_config.tokens[i]);
  return
  tokensHoldings +
  crvLpHoldings +
  (cvxEarningsInFeeToken + crvEarningsInFeeToken);
```

5. Due to the increased _assetPriceCached, the value of 84 zETH increased to 221 zETH.

```
function balanceOf(address account) public view virtual override returns (uint256) {
             if (!containRigidAddress(account)) return super.balanceOf(account);
             return balancesRigid[account];
42
```

```
function convertFromNominalCached(uint256 nominal, Math.Rounding rounding)
             internal
             view
             virtual
             returns (uint256 value)
             if (nominal == type(uint256).max) return type(uint256).max;
71
             return nominal.mulDiv(assetPriceCached(), DEFAULT DECIMALS FACTOR, rounding);
```

```
function assetPriceCached() public view virtual returns (uint256) {
16
             return assetPriceCached;
17
18
```

6. They exchanged the CRV obtained in step 4 back to ETH to repay the flash loan.

```
[call][106470][@] [CurveTricryptoOptimizedWETH]. earthogo(arg0-2, arg1-1, arg5-105829003752209692749877, arg1-0.
                                                                                                                                      mrgi=falre, mrgi=0xA21a2859d80dC42D332F778Cbb9eA127100e5d75) - ()
[call][105401](a) [CurveTricryptoOptimiredWEIR]. orchange(arg)=2. arg)=1. arg)=18060665822920731953797. arg)=0.
                                                                                                                                      argirfalse.
                      (CurveTricryptoOptimizedWETH). michange(urg)*2, urg)*1, urg)*128120409266480321465397.
                                                                                                                                                     arg(-0xA21x2959d80dC42D332F778Cbb9eA127100e5d75) \rightarrow ()
[call][105421][o]
                      {CurveTricryptoOptimizedWEIH}. **change(urgl*2, urgl*1, urgl*142165568349485099351576,
                                                                                                                            A113-0.
                                                                                                                                      argu-false.
                                                                                                                                                     ## ### OxA21 a2B594804C42D332F778Cbb9eA127(00a6476) → ()
[call][105471][m]
                                                                                                                                      m \in (-false, m \in -0xA21a2859d80dC420002F779Cbb9eA127(00e5d75) \rightarrow
                     [CurveTricryptoOptimizedWETH].each.mge(srg0=2, srg1=1, srg2=158657943535631679073667,
[call][[05483][as] [CurveTricryptoOptimizedWETH].eschange(arg0=2,
                                                                                      mrgD=178201625214990230221979,
mrgD=201599470635337503184491,
                                                                                                                                       acquefalre.
                                                                                                                                                     1151-0xA21x2959d80dC420332F778Cbb9+A127100+5d76) \rightarrow ()
                      {CurveTricryptoOptimizedWEIH].exchange(incom2,
                                                                                                                                                     1115 * 0xA21425596804C425332F778Cbb9eA127100e6475) ->
[call] (105453) [c]
                                                                            miglet.
                                                                                                                            1177*0,
                                                                                                                                       argirfalse.
                     {CurveTricryptoOptimizedWETH}.exchange(ing)=2, ingl=1, ingl=229937149571057248476436, ingl=0,
                                                                                                                                      mrg(=false, mrg)=0xA21a2859680dC429332F778Cbb9eA127190e5d75) -> ()
[call][ID5457][e] {CurveTricryptoOptimizedWETH].srchunge(urph=2, urpl=1, urpl=264711810765429950412992, [call][ID48277][e] {CurveTricryptoOptimizedWETH].srchunge(urph=2, urpl=1, urph=308034677188862992786822.
                                                                                                                            Httl=0.
                                                                                                                                      \begin{array}{lll} \text{org}(-\text{false}, & \text{org}(-\text{OxA21a28596106C420332F770Cb59-A127100e5675}) \rightarrow & \text{()} \\ \text{org}(-\text{false}, & \text{org}(-\text{OxA21a28598806C420332F770Cb59-A127100e5675}) \rightarrow & \text{()} \end{array}
                                                                                                                            1112-0.
                                                                                       ### 362960488123241020863655.
                                                                                                                            1113-0.
[call][104189][@] [CurveTricryptoOptimizedWETH].eachange(1190~2,
                                                                                                                                       irgi=false, irgi=0xA21a2B59d80dC42B332F778Cbb9eA12710De5d76) <math>\rightarrow ()
[call][104417][6] [CurveTricryptoOptimizedWEIH]. exchange(urgo-2, argl-1, argh-43404)542320906757486036, argl-0.
                                                                                                                                      seg=false. seg=0xA21a28598808C42D332F778Cbb9eA127L00e5875) - ()
                      (CurveTricryptoOptimizedWETH).exchange(org0=2.
                                                                                       ar=>-528318163814244099088266,
                                                                                                                                                     _{\rm HI} = -0x821x2959d80dC420332F770Cbb9+<math>k127100e5d76 \rightarrow ()
[call[[]04300][m]
                                                                                                                                       segarfalge.
                                                                                                                                                     1115-0xA21x28594804C420332F7T0Cbb9eA12T100e5475) -> ()
[call][103303](s) [CurveTricryptoOptimizedWETH]. exchange (urg0-2, urg1-1, urg1-657120365301129776039806,
                                                                                                                            me3=0.
                                                                                                                                      newl-false.
                      {CurveTricryptoOptimizedWETH}.eschinge(srp=2, srp=1, srp=839699805239177460609252,
                                                                                                                                                     1171 = 0 \times A21 + 2859 + 80 + 60 + 29332 = 778 + 659 + A1271 + 60 + 5475 = ()
                                                                                                                                                     == (3=0xA21x2B59d80dC42D332F778Cbb9eA12710De5d75) -> ()
[call][99385][a) [CurveTricryptsOptimiredNETH], exchange [arg0=2, arg1=1, arg0=11111679799111651646196;
                                                                                                                             angled.
                                                                                                                                       arguefalre.
```

7. They exchanged the increased 221 zETH (LP) for 389 ETH.

[call](:3888) 0xfC89b519658967fCBE1f525f1b0f4bf62d9b9018; exchange()=0. |=1.

```
Tobarda change Compa 0=0x80 3=90f250890faT71c53c981540daf005f63f637f1869fT0T052615a3497140.

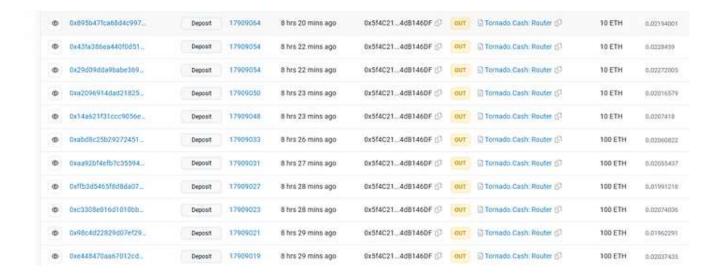
    [call] [DESTE] (♠) [Typer_contract (Oxaff8..e577)]. each

                                         =389796925215820417775, _mim_d;=0) → (389176566178197178266)
 > [call] [NUM] (a) [freETR].trunfeffum(f) == 0x421a18594804(4D323FFT0Cb59x127100x54T5, tr=[Upper_contract (DraifB..x5777)]. === -39979692523582041TT75) → (true) [call] [NL] 0x421a28594804(4D323FFT0Cb59x127100x54T5, tallbank[39, 1765x1781071702x6 ETR] () → (Dr)
   [call] [ht] 0x42; a28594904Ce20332FT79Cb69eA127100e5476.fallb
```

8. They repaid the 6811 ETH flash loan and other fees, resulting in a profit of 26 ETH.

Funds Tracing:

As of the time of writing, the Beosin security analysis team found that the stolen funds had all been transferred to Tornado cash.



Summary:

In response to this incident, the Beosin security team recommends:

- 1. Similar projects should consider different token pool dependencies when calculating LP value.
- 2. Before the launch of a project, it's advisable to engage a professional security auditing company for comprehensive security audits to mitigate security risks.

Beosin is a leading global blockchain security company co-founded by several professors from world-renowned universities and there are 40+ PhDs in the team, and set up offices in 10+ cities including Hong Kong, Singapore, Tokyo and Miami. With the mission of "Securing Blockchain Ecosystem", Beosin provides "All-in-one" blockchain security solution covering Smart Contract Audit, Risk Monitoring & Alert, KYT/AML, and Crypto Tracing. Beosin has already audited more than 3000 smart contracts including famous Web3 projects PancakeSwap, Uniswap, DAI, OKSwap and all of them are monitored by Beosin EagleEye. The KYT AML are serving 100+ institutions including Binance.

Contact

If you need any blockchain security services, welcome to contact us:

Offiial Website Beosin EagleEye Twitter Telegram Linkedin