

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



Beosin · Follow

4 min read · Aug 15



3



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:

Tx1:

0x2aec4fdb2a09ad4269a410f2c770737626fb62c54e0fa8ac25e8582d4b69occa

Tx2:

0x0788ba222970c7c68a738b0e08fb197e669e61f9b226ceec4cab9b85abe8cceb

- Attacker's Address:

0x5f4c21c9bb73c8b4a296cc256cocode324db146df

- Attack Contract:

0xa21a2b59d80dc42d332f778cbb9ea127100e5d75

- 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.


```

279     function lpPrice() public view returns (uint256) {
280         return calcTokenPrice(totalHoldings(), totalSupply());
281     }
282
283     function totalHoldings() public view returns (uint256) {
284         uint256 length = _poolInfo.length;
285         uint256 totalHold = 0;
286         for (uint256 pid = 0; pid < length; pid++) {
287             PoolInfo memory poolInfo_ = _poolInfo[pid];
288             if (poolInfo_.lpShares > 0 && poolInfo_.enabled) {
289                 totalHold += poolInfo_.strategy.totalHoldings();
290             }
291         }
292         return totalHold;
293     }
294
295     function totalHoldings() external view virtual returns (uint256) {
296         uint256 crvLpHoldings = (cvxRewards.balanceOf(address(this)) * getCurvePoolPrice()) /
297             CURVE_PRICE_DENOMINATOR;
298
299         uint256 crvEarned = cvxRewards.earned(address(this)); 1. control crv balance
300         uint256 amountIn = crvEarned + _config.crv.balanceOf(address(this));
301         uint256 crvEarningsInFeeToken = rewardManager.valuate(
302             address(_config.crv),
303             amountIn
304         ); 2. raise crv price by exchanging wETH to crv
305
306         uint256 cvxTotalCliffs = _config.cvx.totalCliffs();
307         uint256 cvxRemainCliffs = cvxTotalCliffs -
308             _config.cvx.totalSupply() /
309             _config.cvx.reductionPerCliff();
310
311         amountIn =
312             (crvEarned * cvxRemainCliffs) /
313             cvxTotalCliffs +
314             _config.cvx.balanceOf(address(this));
315         uint256 cvxEarningsInFeeToken = rewardManager.valuate(
316             address(_config.cvx),
317             amountIn
318         );
319
320         uint256 tokensHoldings = 0;
321         for (uint256 i = 0; i < 3; i++) {
322             tokensHoldings += balanceOfNative(_config.tokens[i]);
323         }
324
325         return
326             tokensHoldings +
327             crvLpHoldings +
328             (cvxEarningsInFeeToken + crvEarningsInFeeToken); 3. eventually more earnings are calculated

```

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

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

```
> [call][0]([e]) { [Wrapped Ether].transfer({to:[Balancer: Vault], val:=68110000000000000000) => (true)} return 6811 ETH  
[staticcall][934]([e]) { [Wrapped Ether].balanceOf([Balancer: Vault]) => (6518023662441133399775)  
[log] FlashLoan(skip:=0xd0d7fde01ab95780adcd1cdcdddc2ee9e3a2042fecbf532836dfb895f, hop_1:=0x000000000000000000000000000000000000a2a2c59480dc42d3232f77bcbb9ea127100e5d75, top_1:=  
[staticcall][029]([e]) { [fxETH].balanceOf(account:=0xfC8B9519A58967CEBE1E52F1B8Fd4bfc6249b9018) => (1045341414037292215)  
[staticcall][030]([e]) {Curve.fi: CRV Token}.balanceOf(arg:=0xA21a2D59480DC42D32F77BCBB9EA127100e5d75) => (0)  
[staticcall][934]([e]) { [Wrapped Ether].balanceOf(0xA21a2D59480DC42D32F77BCBB9EA127100e5d75) => (26336546493759569471)  
> [call][9]([e]) { [Wrapped Ether].withdraw(val:=26336546493759569471) => () earn 26 ETH  
[call][1]([00P9I04...]) {05f4c21e9b7b3e884a29ec2560cd632484146DF.fallback[26, 336546493759569471] ETH}() => (0x)
```

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.

0x895b47fca6d4c997...	Deposit	17909064	8 hrs 20 mins ago	0x5f4C21...4dB146DF	OUT	Tornado.Cash: Router	10 ETH	0.02194001
0x43fa386ea440f0d51...	Deposit	17909054	8 hrs 22 mins ago	0x5f4C21...4dB146DF	OUT	Tornado.Cash: Router	10 ETH	0.0228439
0x29d09dda9babe369...	Deposit	17909054	8 hrs 22 mins ago	0x5f4C21...4dB146DF	OUT	Tornado.Cash: Router	10 ETH	0.02272005
0xa2094914dad21825...	Deposit	17909050	8 hrs 23 mins ago	0x5f4C21...4dB146DF	OUT	Tornado.Cash: Router	10 ETH	0.02016579
0x14ab21f31ccc9056e...	Deposit	17909048	8 hrs 23 mins ago	0x5f4C21...4dB146DF	OUT	Tornado.Cash: Router	10 ETH	0.0207418
0xabd8c25b9272451...	Deposit	17909033	8 hrs 26 mins ago	0x5f4C21...4dB146DF	OUT	Tornado.Cash: Router	100 ETH	0.02060022
0xaa92bf4efb7c35594...	Deposit	17909031	8 hrs 27 mins ago	0x5f4C21...4dB146DF	OUT	Tornado.Cash: Router	100 ETH	0.02055437
0xffb3d5465fd8da07...	Deposit	17909027	8 hrs 28 mins ago	0x5f4C21...4dB146DF	OUT	Tornado.Cash: Router	100 ETH	0.01991218
0xc3308e016d1010bb...	Deposit	17909023	8 hrs 28 mins ago	0x5f4C21...4dB146DF	OUT	Tornado.Cash: Router	100 ETH	0.02074036
0x98c4d22829d07ef29...	Deposit	17909021	8 hrs 29 mins ago	0x5f4C21...4dB146DF	OUT	Tornado.Cash: Router	100 ETH	0.01962291
0xe448470aa67012cd...	Deposit	17909019	8 hrs 29 mins ago	0x5f4C21...4dB146DF	OUT	Tornado.Cash: Router	100 ETH	0.02037435

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:

[Official Website](#) [Beosin](#) [EagleEye](#) [Twitter](#) [Telegram](#) [Linkedin](#)