

A rug pull of \$1.8M, an analysis of zkSync dex Merlin security incident



Beosin · Follow

4 min read · Apr 29

Listen

Share



Image Source: <https://paxful.com/university/what-is-rug-pull-crypto/>

On April 26, according to Beosin EagleEye security situation awareness platform, Merlin Dex was attacked and the funds of USDC-WETH liquidity pool had been drained. The attacker made a profit of about \$1.8M. Beosin security team analyzed the security incident immediately and the details are as follows.

Information related to this incident

Take one of the attack transactions for example to analyze:

The transaction hash:

0xf21bedfb0e40bc4e98fd89d6b2bdaf82f0c452039452ca71f2cac9d8fea29ab2

The addresses of the attacker:

0xcoD6987d10430292A3ca994dd7A31E461eb28182

0x2744d62a1e9ab975f4d77fe52e16206464ea79b7

The attacked smart contract:

0x82cf66e9a45Df1CD3837cF623F7E73C1Ae6DFf1e (USDC-WETH Pool)

The attack process

1. The pool creator/the attacker (0xcoD6987d10430292A3ca994dd7A31E461eb28182) created MerlinSwapFactory contract (0x63E6fdAdb86Ea26f917496bEEEEAEa4efb319229F) and during the initialization the Feeto address had been set to 0xcoD6987d10430292A3ca994dd7A31E461eb28182, the attacker address.



2. The attacker deployed USDC-WETH pool (0x82cf66e9a45Df1CD3837cF623F7E73C1Ae6DFf1e) by MerlinSwapFactory contract. Here we can see that USDC and WETH of the pool were approved max amount for the Feeto address during the initialization. It is obvious that there is a centralization risk in the contract.

```

82 function initialize(address _token0, address _token1) external {
83     require(msg.sender == factory && !initialized, 'MerlinSwapPair: FORBIDDEN');
84     // sufficient check
85     token0 = _token0;
86     token1 = _token1;
87     IERC20(token0).approve(IMERlinSwapFactory(factory).feeTo(), type(uint256).max);
88     IERC20(token1).approve(IMERlinSwapFactory(factory).feeTo(), type(uint256).max);
89
90     precisionMultiplier0 = 10 ** uint(IERC20(_token0).decimals());
91     precisionMultiplier1 = 10 ** uint(IERC20(_token1).decimals());
92
93     initialized = true;
94 }

```

3. Because of max amount approval of USDC and WETH for Feeto address, the attacker transferred all the tokens in the pool.

From [0xc0D6987d10430292A3ca994dd7A31E461eb28182](#)

Tokens Transferred From [L2 0x82cf66e9a45...Ff1e](#) to [L2 0x2744D62a1e9...79b7](#) for 811295.747611 USDC

From [L2 0x000000000000...8001](#) to [L2 0xc0D6987d104...8182](#) for 0.00026027 ETH

From [L2 0x000000000000...8001](#) to [L2 0xc0D6987d104...8182](#) for 0.00326185475 ETH

Contract address [0x3355df6D4c9C3035724Fd0e3914dE96A5a83aaf4](#)

4. It is worth noting that the owner and Feeto address of the factory contract were changed to another address before the rug pull. However, the change was unnecessary to make the rug pull. We guess that it was a step the attacker took to confuse people.

From [0xc0D6987d10430292A3ca994dd7A31E461eb28182](#)

Tokens Transferred From [L2 0x000000000000...8001](#) to [L2 0xc0D6987d104...8182](#) for 0.000169237 ETH

Contract address [0x63E6fdAdb86Ea26f917496bEEFAEa4efb319229F](#)

Input data [Show original input](#)

[View decoded](#)

Function: setFeeTo(address _feeTo)

#	NAME	TYPE	DATA
0	_feeTo	address	0xb17e8F99f71d83cbF500911ee8705Dc255E2dA83

From [0xc0D6987d10430292A3ca994dd7A31E461eb28182](#)

Tokens Transferred From [L2 0x000000000000...8001](#) to [L2 0xc0D6987d104...8182](#) for 0.00025340275 ETH

Contract address [0x63E6fdAdb86Ea26f917496bEEFAEa4efb319229F](#)

Input data [Show original input](#)

[View decoded](#)

Function: setOwner(address _owner)

#	NAME	TYPE	DATA
0	_owner	address	0xb17e8F99f71d83cbF500911ee8705Dc255E2dA83

The funds in the USDC-WETH liquidity pool were drained and the attacker made a profit of about \$1.8M.

Vulnerability Analysis

This attack took advantage of the centralization issue of the pair contract. During the initialization, the Feeto address in the factory contract was approved to control all the funds in the USDC-WETH pool, which caused that all the funds in the contract can be drained by the Feeto address.

Funds Tracing

The attacker called the transferFrom function to transfer 811K \$USDC from the pool to 0x2744d62a1e9ab975f4d77fe52e16206464ea79b7.

0xcE4ee0E01bb729C1c5d6D2327BBoF036fA2cE7E2 extracted 435.2 \$ETH from the token1 contract (WETH) and used Anyswap to bridge the funds to 0xa7D481944730a88B862eB57248Cb1B2C8aa358Ad and 0x0b8a3ef6307049aa0ff215720ab1fc885007393d on the Ethereum mainnet, making a total profit of about \$1.8 million.

Up till now, the Beosin KYT AML analysis platform found that the stolen funds are still stored on 0xa7D481944730a88B862eB57248Cb1B2C8aa358Ad and 0x0b8a3ef6307049aa0ff215720ab1fc885007393d. We will continue to monitor and track the stolen funds.

TAROT	Sent: 307,132.00 Received: 306,685.07	zkSync Era Mainnet 0xbaea...02eb	Ethereum Mainnet 0x906e...343f	4 hours 10 mins	Success
USDC	Sent: 45,230.20 Received: 45,190.20	zkSync Era Mainnet 0x60e6...eef4	Ethereum Mainnet 0x9f33...68a4	4 hours 17 mins	Success
USDC	Sent: 70,000.00 Received: 69,960.00	zkSync Era Mainnet 0x7666...23b1	Ethereum Mainnet 0xcce4...71f0	4 hours 20 mins	Success
USDC	Sent: 70,000.00 Received: 69,960.00	zkSync Era Mainnet 0x431a...88ab	Ethereum Mainnet 0xd0d3...7971	4 hours 26 mins	Success
USDC	Sent: 70,000.00 Received: 69,960.00	zkSync Era Mainnet 0x7a33...cc14	Ethereum Mainnet 0xde8c...d193	4 hours 32 mins	Success
USDC	Sent: 70,000.00 Received: 69,960.00	zkSync Era Mainnet 0x8de7...84a8	Ethereum Mainnet 0x0d81...8477	4 hours 41 mins	Success
USDC	Sent: 70,000.00 Received: 69,960.00	zkSync Era Mainnet 0x264f...862e	Ethereum Mainnet 0x57c2...3608	4 hours 46 mins	Success
USDC	Sent: 70,000.00 Received: 69,960.00	zkSync Era Mainnet 0x4865...02c7	Ethereum Mainnet 0xd509...1742	4 hours 53 mins	Success
USDC	Sent: 70,000.00 Received: 69,960.00	zkSync Era Mainnet 0xbf9a...beb3	Ethereum Mainnet 0xfe00...955b	5 hours 0 mins	Success
USDC	Sent: 70,000.00 Received: 69,960.00	zkSync Era Mainnet 0x55b2...dd59	Ethereum Mainnet 0x26f8...9b58	5 hours 7 mins	Success
USDC	Sent: 70,000.00 Received: 69,960.00	zkSync Era Mainnet 0x20b2...d64c	Ethereum Mainnet 0xe9bc...4593	5 hours 11 mins	Success
USDC	Sent: 70,000.00 Received: 69,960.00	zkSync Era Mainnet 0x280e...9772	Ethereum Mainnet 0x617c...cfd1	5 hours 17 mins	Success
USDC	Sent: 50,000.00 Received: 49,960.00	zkSync Era Mainnet 0x5d70...d2a6	Ethereum Mainnet 0x9f0a...2f8c	5 hours 24 mins	Success
USDC	Sent: 50,000.00 Received: 49,960.00	zkSync Era Mainnet 0x01ff...6aad	Ethereum Mainnet 0x8868...8915	5 hours 32 mins	Success

USDC	Sent: 18,744.10 Received: 18,704.10	zkSync Era Mainnet 0xd80a...cfad	Ethereum Mainnet 0xff1c...521d	2 hours 53 mins	Success
USDC	Sent: 75,000.00 Received: 74,960.00	zkSync Era Mainnet 0xeb20...96f8	Ethereum Mainnet 0xf311...26bf	3 hours 1 mins	Success
USDC	Sent: 75,000.00 Received: 74,960.00	zkSync Era Mainnet 0xacdf...fee1	Ethereum Mainnet 0x7f7c...1992	3 hours 12 mins	Success
USDC	Sent: 75,000.00 Received: 74,960.00	zkSync Era Mainnet 0xaedc...1693	Ethereum Mainnet 0x475c...d85a	3 hours 20 mins	Success
USDC	Sent: 75,000.00 Received: 74,960.00	zkSync Era Mainnet 0x6b84...66b1	Ethereum Mainnet 0x3f1f...8ea4	3 hours 34 mins	Success
USDC	Sent: 67,500.00 Received: 67,460.00	zkSync Era Mainnet 0xcfd5...266f	Ethereum Mainnet 0xd73...1ab2	3 hours 42 mins	Success
USDC	Sent: 7,500.00 Received: 7,460.00	zkSync Era Mainnet 0xa447...9322	Ethereum Mainnet 0x7e31...9d83	3 hours 50 mins	Success
USDC	Sent: 75,000.00 Received: 74,960.00	zkSync Era Mainnet 0x6539...6930	Ethereum Mainnet 0xfbac...2281	4 hours 1 mins	Success
USDC	Sent: 70,000.00 Received: 69,960.00	zkSync Era Mainnet 0x883c...a03a	Ethereum Mainnet 0xf18d...5da5	4 hours 13 mins	Success
USDC	Sent: 70,000.00 Received: 69,960.00	zkSync Era Mainnet 0xb30d...af16	Ethereum Mainnet 0xe348...2cbe	4 hours 21 mins	Success
USDC	Sent: 70,000.00 Received: 69,960.00	zkSync Era Mainnet 0x607b...45de	Ethereum Mainnet 0x7704...870f	4 hours 29 mins	Success
USDC	Sent: 70,000.00 Received: 69,960.00	zkSync Era Mainnet 0x4349...1e66	Ethereum Mainnet 0x4af1...2b38	4 hours 37 mins	Success

USDC	Sent: 65,558.10 Received: 65,518.10	zkSync Era Mainnet 0x61f6...5054	Ethereum Mainnet 0x79db...5670	4 hours 39 mins	Success
USDC	Sent: 26,259.05 Received: 26,219.05	zkSync Era Mainnet 0x8dd7...8a9c	Ethereum Mainnet 0xb2c8...7a00	5 hours 13 mins	Success
USDC	Sent: 50,000.00 Received: 49,960.00	zkSync Era Mainnet 0xcb63...68b0	Ethereum Mainnet 0x5cf7...c3f8	5 hours 23 mins	Success
USDC	Sent: 50,000.00 Received: 49,960.00	zkSync Era Mainnet 0xe9cf...91ac	Ethereum Mainnet 0x83d1...4206	5 hours 32 mins	Success

Conclusion

From the analysis of Merlin rug pull, we suggest that Web3 projects should use multisig wallets or DAO governance to manage addresses which have control of community treasury and users should watch out the risks of a new project before aping in.

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. It has offices in Singapore, Korea, Japan, and other 10+ countries. 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 and protected more than \$500 billion funds of our clients. You are welcome to contact us.