Exploits and CREATE2 example

Recent Exploits

Arbix Finance - $10M

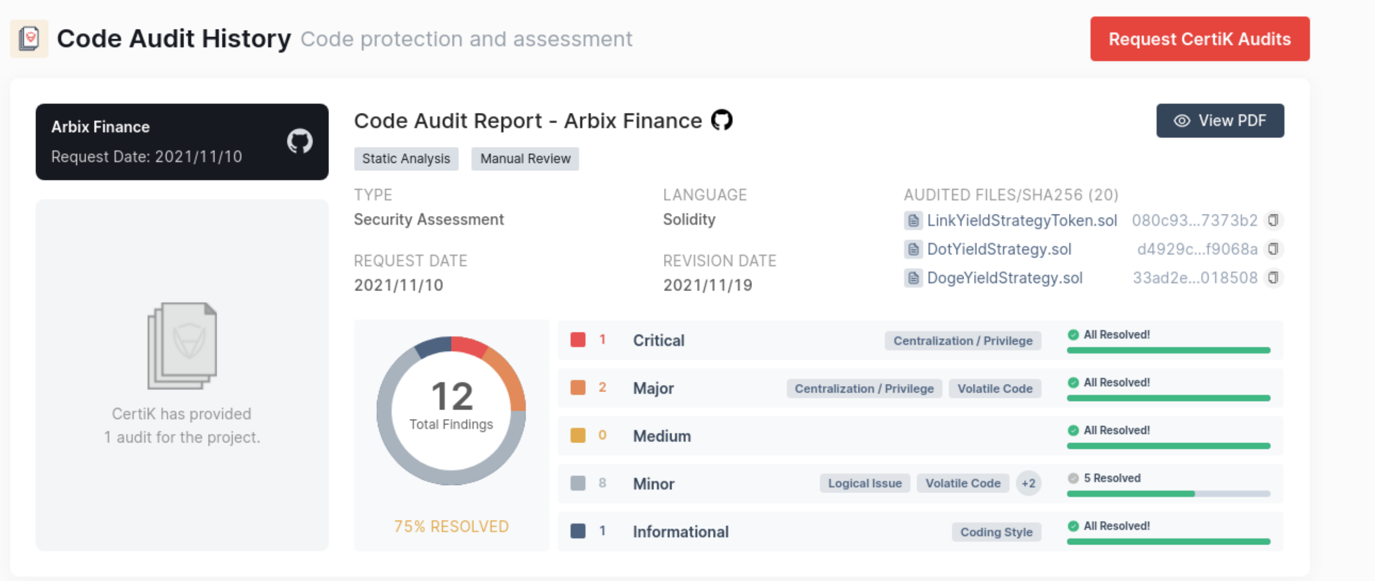
A Rug pull on BSC - around $10M in user’s assets were drained directly from the vaults into a wallet, beginning with ~$1M in BTCB.

Also stolen were:

$920k Binance-pegged ETH
$2.25M in BSC-USD
$1.7M BUSD
$1.4M CAKE
$1M BSC-USDC

In addition to the vault funds, on the 10th December minted 4.5M ARBX was minted. Once the rug pull had begun, these tokens were dumped via PancakeSwap, tanking the price from $1.42 to ~$0.00. The ~$50k in proceeds were then sent to the main rug wallet.

Audit



Code Audit History Code protection and assessment

Arbix Finance
Request Date: 2021/11/10

CertiK has provided
1 audit for the project.

Code Audit Report - Arbix Finance

TYPE
Security Assessment

LANGUAGE
Solidity

REQUEST DATE
2021/11/10

REVISION DATE
2021/11/19

AUDITED FILES/SHA256 (20)

LinkYieldStrategyToken.sol	080c93...7373b2
DotYieldStrategy.sol	d4929c...f9068a
DogeYieldStrategy.sol	33ad2e...018508

12
Total Findings

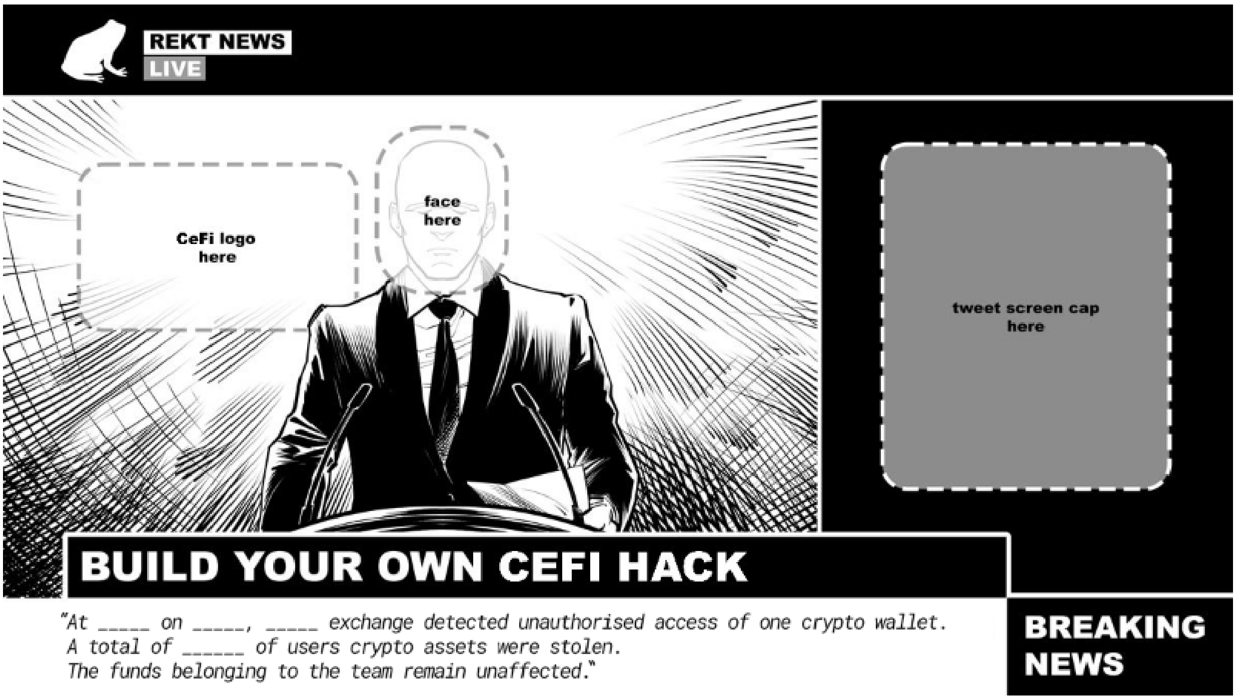
75% RESOLVED

🟥	1	Critical	Centralization / Privilege	All Resolved!
🟧	2	Major	Centralization / Privilege Volatile Code	All Resolved!
🟨	0	Medium		All Resolved!
■	8	Minor	Logical Issue Volatile Code +2	5 Resolved
■	1	Informational	Coding Style	All Resolved!

https://www.certik.com/projects/arbix (https://www.certik.com/projects/arbix)

CEX Hot wallet exploits continue

LCX (https://rekt.news/lcx-rekt/) - $7.9M stolen


REKT NEWS
LIVE
CeFi logo here
face here
tweet screen cap here
BUILD YOUR OWN CEFI HACK
"At _____ on _____, _____ exchange detected unauthorised access of one crypto wallet.
A total of ______ of users crypto assets were stolen.
The funds belonging to the team remain unaffected."
BREAKING NEWS

CREATE2 Problem

```
function pairFor(
address factory,
address tokenA,
address tokenB
) internal pure returns (address pair) {
(address token0, address token1) = sortTokens(tokenA, tokenB);
pair = address(
uint256(
keccak256(
abi.encodePacked(
hex"ff",
factory,
keccak256(abi.encodePacked(token0, token1)),
hex"21cc5acee3cfbef0f72eb490350107dfa223e6ee3abccde30488ff092a96b559" // init c
)
)
)
);
}
```

Test Contract code

````
pragma solidity >=0.6.12;

contract pairTest {
constructor() public {}

event Pair(address);

function pairFor(
    address factory,
    address tokenA,
    address tokenB
) external returns (address pair) {
(address token0, address token1) = tokenA < tokenB
    ? (tokenA, tokenB)
    : (tokenB, tokenA);
pair = address(
uint256(
keccak256(
    abi.encodePacked(
        hex"ff",
        factory,
        keccak256(abi.encodePacked(token0, token1)),
        hex"e18a34eb0e04b04f7a0ac29a6e80748dca96319b42c54d679cb821dca90c6303" /
    )
)
)
);
emit Pair(pair);
}
}
````

~~~
function pairCodeHash() external pure returns (bytes32) {
        return keccak256(type(UniswapV2Pair).creationCode);
    }
    ```
~~~