INVESTIGATIVE
INTELLIGENCE REPORT

Project Name:

Unicorn Nodes

ASSURE DEFI™
THE VERIFICATION **GOLD STANDARD**

Project Name:

Unicorn Nodes

Project Name: **Unicorn Nodes**
Blockchain: **AVALANCHE**
Token (If Applicable): **$RNBW**

Token Contract Address:
0x388089e67B864DC76091bdE638bca9e639f9ceCE

Quantity of Responsible Parties w/ Identification on File with **Assure DeFi LLC**: **2**
Nationality of Responsible Parties: **United States & South Africa**

Date Investigation Was Opened:
4/14/2022

Alleged Scam/Fraud Type:
Rugpull, Exploit, Negligence

Roles of Verified Team Members:
Developer (Responsible for the farm, token, sale contracts)
Project Manager/ Social Media Manager

CONTACT INFORMATION FOR LAW ENFORCEMENT TO OBTAIN KYC & IDENTITY DETAIL INFORMATION ON FILE WITH ASSURE DEFI:

Direct Contact
Email: chapo@assureteam.io
Twitter DM: www.twitter.com/el_crypto_chapo/
Telegram DM: https://t.me/el_crypto_chapo/

Mailing Address
Assure DeFi LLC
c/o United States Corporation Agents, Inc
411 Wolf Ledges Parkway, Suite 201
Akron, OH 44311

Estimate of Injured Parties:
< 500

Estimate Funds Stolen:
~$130,000

Last Known Location of Funds:
Tornado.cash

***See details below in BlockChain Forensics/Funds Tracing Section of Report.**

BACKGROUND INFORMATION

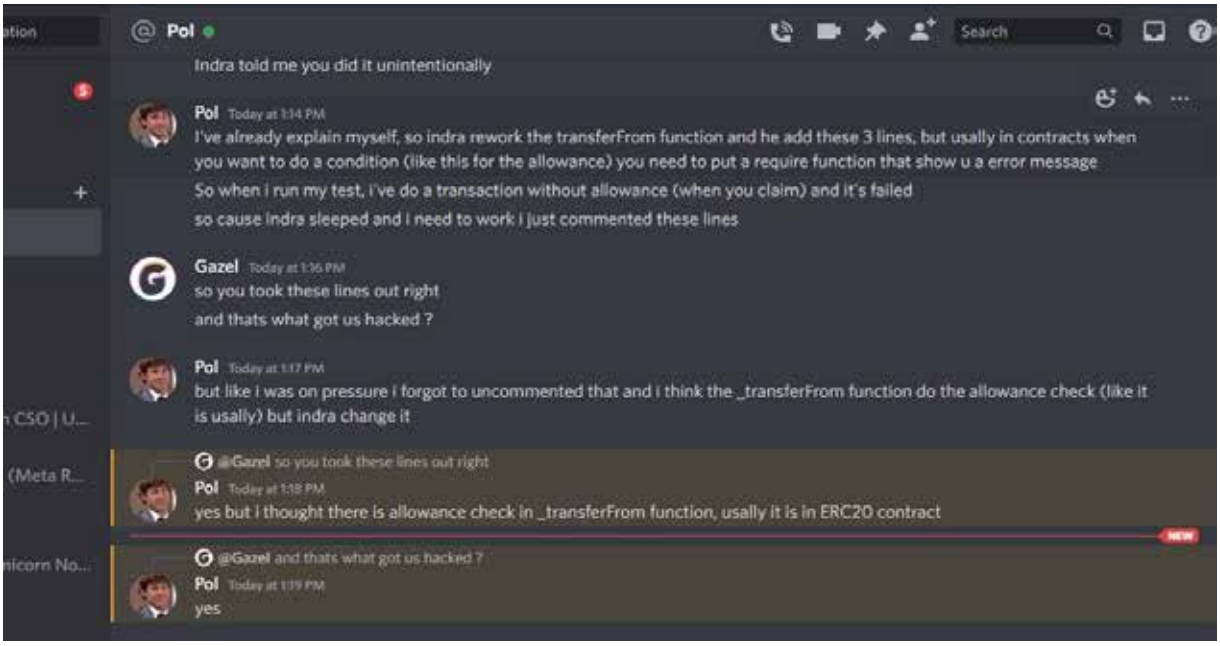
Unicorn Nodes was a node project on Avalanche which promised high rewards.

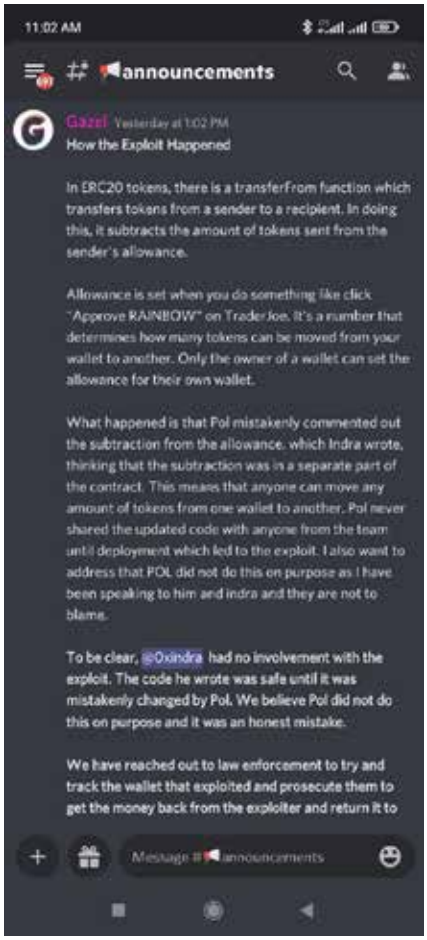
The project was launched on 4/13/2022 and was trading for only a matter of hours before the liquidity was removed and the price dropped quickly from its ATH at around $16 to where it sits now at $0.007.

When reaching out to the primary contact for the team, it was claimed that an exploit had happened via the deployer. He explained that he believed that they were exploited through the contracts that had been deployed by the developer they had hired from M.O.D. It was claimed that it was caused by the developer leaving out/commenting out 3 lines of code which left the contract vulnerable to attack. It was believed that whoever had exploited the contract had stolen just under $130k in total.

SCREENSHOTS OF HIS CONVERSATIONS WITH THE DEV WERE PROVIDED AS EVIDENCE.(BELOW)

BACKGROUND INFORMATION CONT.



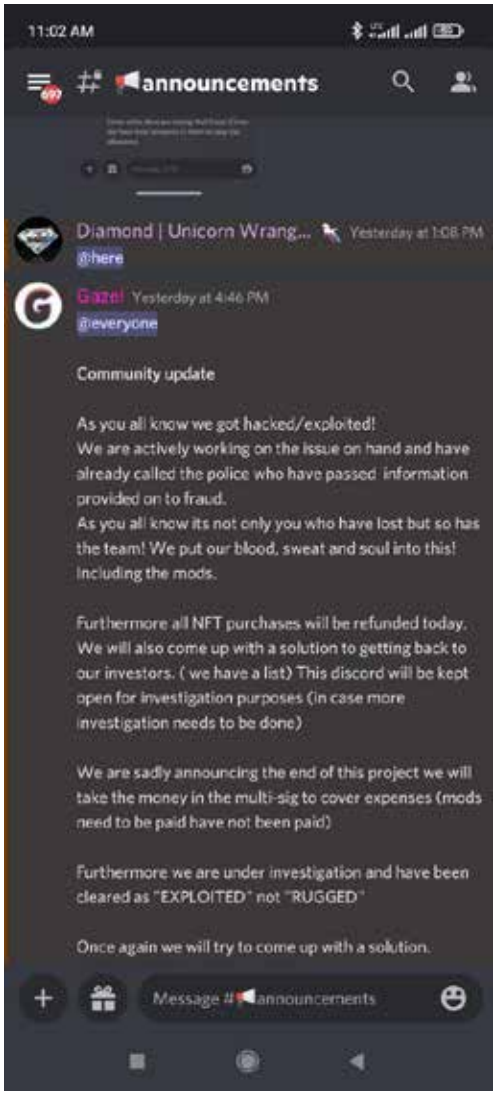


BACKGROUND INFORMATION CONT.

A timeline of the supposed events were also provided by the Unicorn Nodes primary contact we were in communication with.

- Nodemaster the main dev left shortly before launch (dad died). and even though contract was audited it has since been updated to fix the flash loan exploit and add other functions.
- Pol was contracted through M.O.D.? and 0xindra was also recruited to work on it
- Contracts weren't ready for launch day so it was pushed back 24 hours.
- Launch day, Indra hands it off to POL in good shape, POL makes changes and comments out code to resolve some errors
- Launch was not good and showed POLs inexperience.
- Contract was exploited and the liq was emptied by a hacker

The team provided plans for attempting to reimburse some of the community and staff members by deciding to allocate the funds of the treasury to go towards refunding NFT holders and using what was left in the multisig to pay mods who had yet to receive pay.



ATTACK INITIATOR ADDRESS FLOW:

(1) Attacker address withdrew 0.1 ETH Tornado.cash note
(2) Bridged 0.04 WETH with Avalanche Bridge
(3) Received 0.039 WETH from Avalanche Bridge
(4) Swapped 0.039 WETH to 1.49 AVAX on Trader Joe
(5) Created a smart contract (0x5ca2162900708dcad475ff677bf83da105b278a6)
(6) Called 0xeb961914 function selector on the smart contract, which drained the trading pair funds on treasury's behalf, receiving ~129,982 USDC.

The funds are located on treasury contract which is a Gnosis Safe multisignature wallet, but the transferFrom function was overwritten with a code ignoring the allowance check.

```
function transferFrom(address sender, address recipient, uint amount) public virtual override returns (bool) {
    if (msg.sender == farm) {
        _transfer(sender, recipient, amount);
        return true;
    }
    /* if (_allowances[sender][msg.sender] != type(uint256).max) {
        _allowances[sender][msg.sender] = _allowances[sender][msg.sender] - amount;
    } */
    return _transferFrom(sender, recipient, amount);
}
```

transferFrom call:


```
{
  "[OPCODE]": "CALL",
  "from": {
    "address": "0x5ca2162900708dcad475ff677bf83da105b278a6",
    "balance": "0"
  },
  "to": {
    "address": "0x388089e67b864dc76091bde638bca9e639f9cece",
    "balance": "0"
  },
  "value": "0",
  "[INPUT]":
"0x23b872dd000000000000000000000000061d81f1a64af876d14c346aca3c8eb6f0ecf78650000000
0000000000000000042e39db101fe319ccc249a243b0c9e75938c123500000000000000000000000000
0000000000000000000013eca7fe652a6b9a0000",
  "[OUTPUT]":
"0x0000000000000000000000000000000000000000000000000000000000000001",
  "gas": {
    "gas_left": 234630,
    "gas_used": 123594,
    "total_gas_used": 79974
  }
}
```

THE INPUT DECODES TO:

transferFrom(0x61D81F1A64af876D14c346Aca3C8eb6f0Ecf7865,
0x42e39db101fe319ccc249a243b0c9e75938c1235, 9409050000000000000000)

(7) Called clean() (0xfc4333cd selector) function that self destructed the contract
(8) Bridged 129,982 USDC to Ethereum
(9) Received 129,910 USDC in the Ethereum Network
(10) Swapped 129,910 USDC to 42.06 ETH on Uniswap
(11) Deposited 41.8 ETH to Tornado.cash:

10 ETH transactions

https://etherscan.io/tx/0x42f6d683b7ff6a544032cec2f3e707479868d85b58d572d4a711d976e8dc8814
https://etherscan.io/tx/0x15ca6bc7fcdea86cf59c819a233c81b8c10247201b454ab55500202a678bc436
https://etherscan.io/tx/0xf226a541ec7093eed82ea6132e508b090faaf0728074f3ebf1cfc6adf8a9a40e
https://etherscan.io/tx/0xba7e73f3ce61ab7fa26a6c07b66806308109fef025fbae5088377fc90b7a0425

1 ETH transactions

https://etherscan.io/tx/0xcde79b7a707ef084e7cf027cd902f85d6416acc09626b2fd2b34bd962171dac2

0.1 ETH transactions

https://etherscan.io/tx/0x6dfb4ef74493086843ab333de0568661732dd0917fe6f4f418805c08cd11df6f
https://etherscan.io/tx/0x26703f5ed21b5ed752c5d7d4f52eeb1f914789e95947e38a09cbe4cd1c54fabe
https://etherscan.io/tx/0x80651bb0b2d4a9752171cea169d4135c69d5db2932ee08436c0cfd54b369cbb0
https://etherscan.io/tx/0x9e963c22b0dca81b701a3bec0d6f54f525251d2b03326ef42e8afb7777dbb7ba
https://etherscan.io/tx/0xca1b64f84b2542d64f188b12098a578c9f24a3a7880c2f4aba24b774c26e0604
https://etherscan.io/tx/0x64b4ceede8e571ec7ca44a8fddd9c88b922ea4ee1bb62cc7b1dfcb13275f4818
https://etherscan.io/tx/0x88118a47fb4110099c1177d0171603d960bfb93c367ec1e8687305215ebb966d

Supplemental Information

(Unverified by Assure, Provided by 3rd Party Partner)
Breakdown of the Unicorn Nodes exploit.

1) A v2 migration of the code occurred on 4/13/2022 and was announced on their discord at 9:18PM.

2) The original code was written by 0xIndra, a trusted Dev in the community, and the Founder and Dev of Etherstones. The original code contained four lines, lines 833-836, which check the sender's allowance during a transaction. In the V2 migration, these lines were commented out. This essentially allows an exploiter to transfer any number of $RNBW tokens from any wallet to any other wallet. You can see in the code that these lines were commented out in the migration, and that the audit by Spade Solidity did not note this issue on the V1 contract. This issue was not present in the V1 migration during code checks by the CN Smart Contract Team.

3) On Apr 14th 06:02:45 AM, an unknown wallet exploited the newly created vulnerability, and transferred 5,432 RNBW, which they sold for 129,982.51 USDC the Trader Joe DEX.

SUMMARY/CONCLUSION

Based on the information gathered regarding the case, experts concluded that the transferFrom function was vulnerable by itself, and, in this case, the treasury being a multisignature wallet wouldn't help with ERC20 tokens. Thus, anyone had the opportunity to conduct the attack, but it is important to note that commenting out the allowances in the transferFrom function directly leads to vulnerable scenarios and is not a common practice.

Experts also attempted to trace the funds from Tornado.cash. Given the big anonymity sets for ETH deposits, no exact matches were found.

The attacker could not be identified through the investigative process. There are claims of negligence by the project team, that they were warned about this exploit path prior to launch and ignored them without addressing the code deficiencies.

Unicorn nodes have declared they will be (partially) refunding holders of NFTs from the treasury wallet. What's left in the multisig has been designated to be used for covering costs which include the pay of unpaid mods.

The decision was made by the Unicorn node team to close down the project. As of the time of this writing, their Twitter account has been deleted. The community Discord server is still active.

RECOMMENDED ACTION ITEMS/NEXT STEPS FOR ADVERSELY AFFECTED PARTIES

Any wallets that contain any amount of $RNBW tokens are potentially subject to the exploit as it is currently still live. We recommend revoking all permissions for this contract using a site like https://revoke.cash (or others) to ensure no further losses occur.

File law enforcement reports with the following agencies:

#1: **Federal Trade Commission | http://www.reportfraud.ftc.gov/**

#2: **Commodity Futures Trading Commission | http://www.cftc.gov/Complaint**

#3: **U.S. Securities and Exchange Commission | https://www.sec.gov/tcr**

NEXT STEPS FOR ASSURE

- **Assure will file a report with the IRS-CI (Internal Revenue Service - Criminal Investigation)**
- **Assure will provide guidance on additional appropriate jurisdictions & agencies to which injured parties can file reports as applicable.**
- **Fully cooperate with law enforcement agencies upon official requests as received**

RESOURCES

If you have additional information related to this case, please submit via Assure DeFi's scam reporting form using the following link:

https://www.assuredefi.io/scam-reporting-form

Contact Assure DeFi directly via the following channels:

Twitter Direct Message:
www.twitter.com/assuredefi/
Email: chapo@assuredefi.io

ASSURE DEFI™

THE VERIFICATION **GOLD STANDARD**