// HALBORN

THORChain

Incident Analysis

Prepared by: **Halborn**

Date of Engagement: **July 23, 2021 - July xx, 2021**

Visit: **Halborn.com**

DOCUMENT REVISION HISTORY

VERSION	MODIFICATION	DATE	AUTHOR
0.1	Document Creation	7/22/2021	Gokberk Gulgan
0.2	Document Edits	7/23/2021	Steven Walbroehl
0.9	Document Edits	7/23/2021	Gokberk Gulgan
1.0	Document Final	7/23/2021	Steven Walbroehl

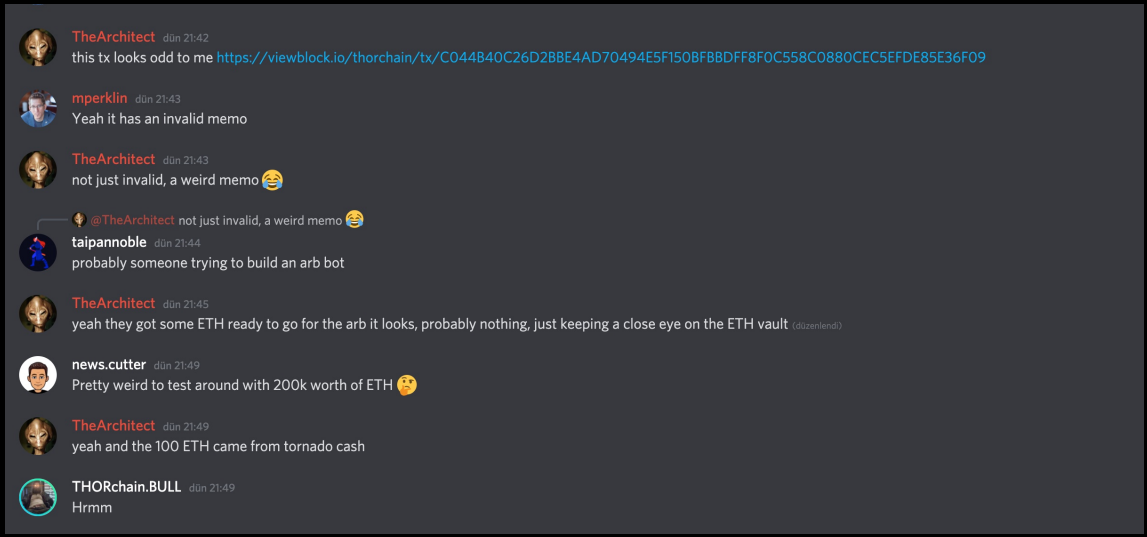
CONTACTS

CONTACT	COMPANY	EMAIL
Rob Behnke	Halborn	@HalbornSecurity on twitter
Steven Walbroehl	Halborn	@HalbornSteve on twitter

INCIDENT ANALYSIS

1.1 TECHNICAL ANALYSIS

An attacker targeted Thorchain Bifrost component through ETH Router contract. The observation of an attack began on the 22.07.2021 - 21:42 GMT +3. TheArchitect observed transaction which shows unintended behaviour.



An attacker created contract which is available on the https://etherscan.io/address/0x700196e226283671a3de6704ebcdb37a76658805. After the decompilation of the contract, It has been observed that an attacker created a function which is interacting with Thorchain ETH Router.

Listing 1: An Attacker Contract

```
else:
    require ext_code.size(0
        xc145990e84155416144c532e31f89b840ca8c2ce)
    static call 0xc145990e84155416144c532e31f89b840ca8c2ce.0
        x3b6a673 with:
            gas gas_remaining wei
           args 0xf56cba49337a624e94042e325ad6bc864436e370, addr
              (_param1)
    if not ext_call.success:
        revert with ext_call.return_data[0 len return_data.size]
    require return_data.size >= 32
    require ext_call.return_data == ext_call.return_data[0]
    if ext_call.return_data and 9 > -1 / ext_call.return_data
```

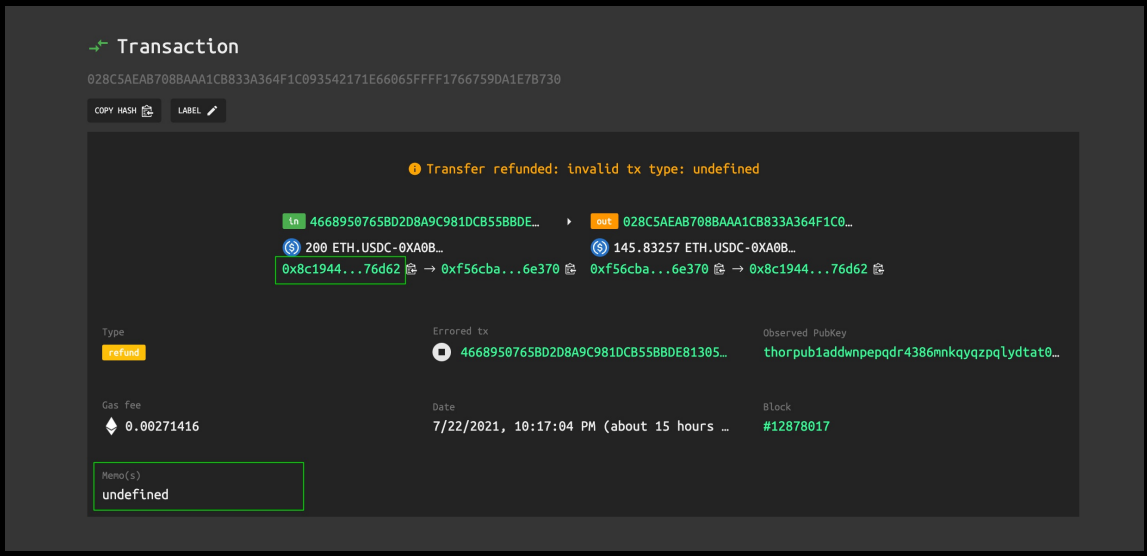
```
            [0]:
11           revert with 'NH{q', 17
12       stor1 = addr(_param1)
13       stor2 = 9 * ext_call.return_data / 10
```

During the transactions, the following addresses are seen in the transactions.

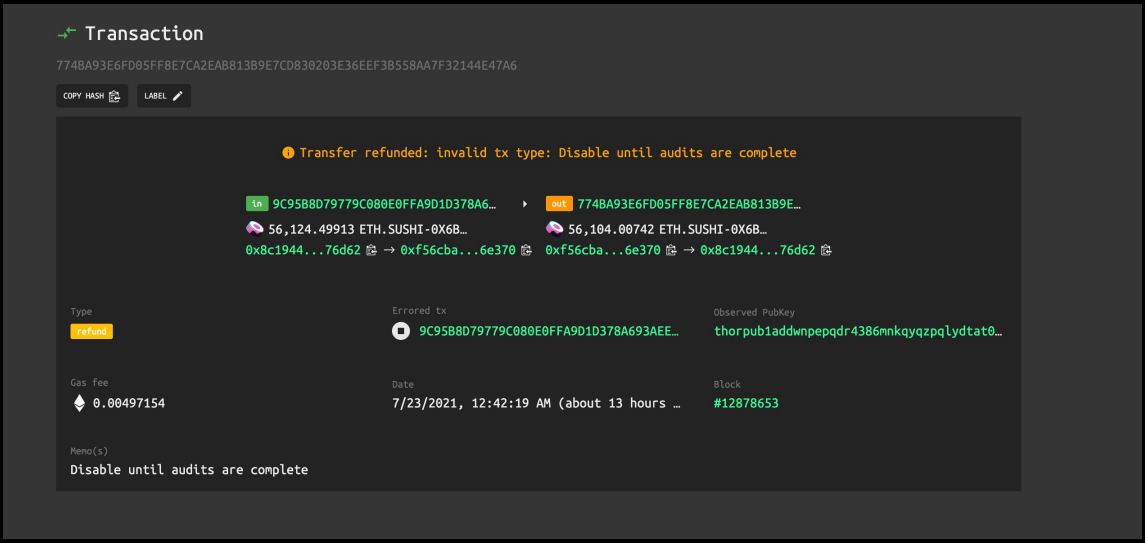
Listing 2: An Attacker Address Details

```
1 0xc145990e84155416144c532e31f89b840ca8c2ce router,
2 0xf56cba49337a624e94042e325ad6bc864436e370 vault,
3 0x700196e226283671a3de6704ebcdb37a76658805 attack contract,
4 0x8c1944fac705ef172f21f905b5523ae260f76d62 attack wallet (spawned
      from Tornado Cash)
```

According to an analysis of the transactions, the attacker tried to send invalid memo field to Thorchain Bifrost component.



Transactions to THORChain pass user-intent with the MEMO field on the chains which contain custom user input. The THORChain inspects the transaction object, as well as the MEMO in order to process the transaction, so care must be taken to ensure the MEMO and the transaction is valid. If not, THORChain will automatically refund. Reference



Halborn Team noticed that the initial entry point was ETH contract. However, a hacker claimed that it is possible to steal other type coins too. As an conclusion, a hacker was right and It is possible to refund other type coins too.

1.2 ATTACK STEPS

The network was halted during the attack, Refunds and LP withdrawals are still allowed. The attack can be named as Lack of proper multi-event handling. The hacker targeted a refund logic. The simple attack steps can be seen below.

- The attacker created fake router (Contract Address), than a deposit event emitted when the attacker sent ETH.
- The attacker passes returnVaultAssets() with a small amount of ETH, but the router is defined as an Asgard vault.
- On the Thorchain Router, its forwarding ETH to created fake Asgard.
- This creates a fake deposit event with a malicious memo.
- Thorchain Bifrost intercepts as a normal deposit and refunds to an attacker due to a bad memo definition.

1.3 ECONOMICAL OBSERVATIONS

Impact (~$8M USD)

966.62 ALCX

20,866,664.53 XRUNE

1,672,794.010 USDC

56,104 SUSHI

6.91 YEARN

990,137.46 USDT

1.4 TRANSACTIONS

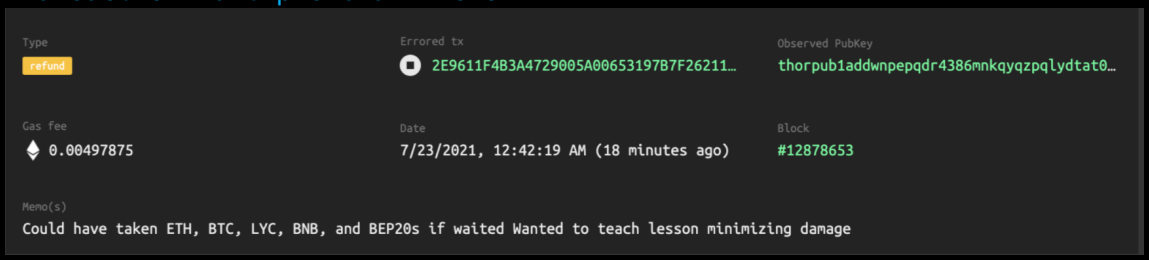
- Contract Address
- Transaction 1
- Transaction 2
- Transaction 3
- Transaction 4
- Transaction 5
- Transaction 6
- Last Transaction By An Attacker

1.5 ATTACKER MEMOS

During the analysis of the incident, Halborn also noticed that messages were left in the memo indicating that further funds could have been withdrawn than the ~$8M USD currently liquidated. Several transactions made by the attacker include:

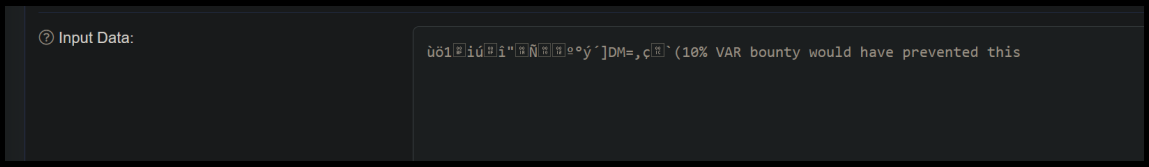
Could have taken ETH, BTC, LYC, BNB, and BEP20s if waited Wanted to teach lesson minimizing damage.

Transaction Multiple Chain Memo



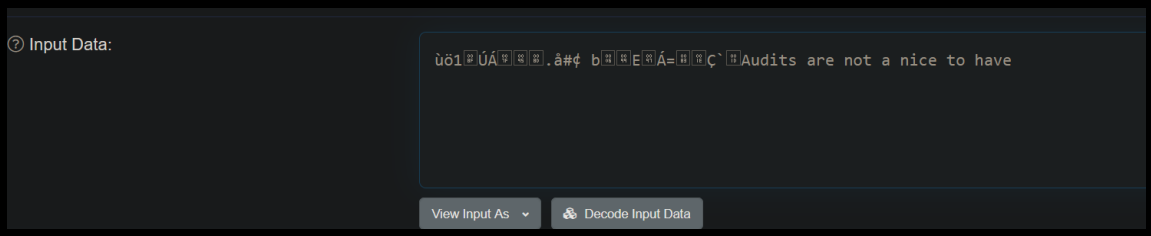
One transaction memo states that only 10% of the total value that could have been extracted was actually stolen. This indicates that the risk persists, and remediation should be made to prevent further loss.

Transaction %10 VAR



Another message is added eluding to THORchain to perform further auditing of their code, indicating that the attacker seems to be trying to teach a lesson to the development team. As of July, THORChain is actively participating in several audits, and security improvements are being made by multiple firms.

Transaction Audit Memo


Input Data:
ùö1ÚÁ.â#¢ bE Á= Ç` Audits are not a nice to have
View Input As
Decode Input Data

1.6 FIXES

- The Bifrost component is configured according to parse transaction which is only emitted from THORChain Router. Commit
- Multiple Events are rejected in the one transaction. Commit

Halborn Team proposes the following recommendations.

- The Router contract should have pause/unpause functionality on the unintended behaviours. Implement a mechanism that can temporarily stop the critical functionalities.
- The white-listing mechanism should implement on the every Bifrost component events.
- Enable Automatic Solvency Checker on the ETH transactions.
- Only Router emitted events should parse from the component therefore an attacker surface will minimized with this action.
- When smart contracts are deployed into the Ethereum blockchain, they are immutable and therefore, not upgradable. In the white-listing progress, router should be placed behind the proxy.
- Implement a policy for tracking new bugs.
- The monitoring should be added into the components. This component should monitor activity using the events.
- Documentation should define all trust boundaries in the components. All counter-measure mechanisms should be defined on the attack vectors.

THANK YOU FOR CHOOSING

// HALBORN