Weekly Blockchain Security Watch

(Aug 14 to Aug 20)

From August 14, 2023 to August 20, 2023, all security incidents that had occurred can be categorized into **Security Hacks and Rug-pulls.**

SECURITY HACKS:

1. **Social Media Accounts Compromised**

From August 14 to August 20, the following social media accounts were compromised and phishing links might be sent in these accounts:

Discord servers of Ceramic@ceramicnetwork, ElmonX@elmonx_official, Rodeo@Rodeo_Finance, Saga@Sagaxyz__ and Pira Finance@PiraFinance

X account of Metis@MetisDAO

2. **Zunami Protocol Suffers Exploit**

On August 14, an ETH deployed DeFi application Zunami Protocol was reported to suffer an exploit.

Basically the protocol suffered an exploit via a flash-loan attack, resulting in a loss of 1,178 ETH. During this attack, the attacker manipulated the price of StakeDAO on Sushiswap using a flash loan. The attacker then cashed out all the stolen funds via Tornado Cash.

The attacker's address is 0x5f4C21c9Bb73c8B4a296cC256C0cDe324dB146DF on Ethereum

Crypto assets worth around US $2.16 million were exploited in this incident.

3. **Rocket Swap Suffers Exploit**

On August 15, a Base deployed application Rocker Swap suffered an exploit.

The attacker’s address is 0x96c0876F573e27636612CF306C9db072d2B13DE8 on Ethereum.

471 ETHs worth around US $868,000 were exploited in this incident.

4. **Harbor Protocol Suffers Exploit**

On August 19, a Cosmos deployed application Harbor Protocol suffered an exploit.

The attacker's address is comdex1sma0ntw7fq3fpux8suxkm9h8y642fuqt0ujwt5 on Cosmos.

Some funds in the application's vaults of stOSMO, LUNA and WMATIC were drained.

5. **Exactly Protocol Suffers Exploit**

On August 19, an OP deployed application Exactly Protocol suffered an exploit.

Basically the application's DebtManager periphery contract was manipulated. The attacker bypassed its permit check, and executed a malicious deposit function to steal assets.

The attacker's addresses are 0x3747dbbcb5c07786a4c59883e473a2e38f571af9 and 0xe4f34a72d7c18b6f666d6ca53fbc3790bc9da042 on OP.

Crypto assets worth around US $7.3 million were exploited in this incident.

RUG-PULLS:

1. **Swirl Lend Rug-pulls**

On August 16, a Based deployed DeFi application Swirl Lend was confirmed to be a rug-pull.

Crypto assets worth around US $462,600 were exploited in this incident.

CONCLUSION-

11 notable security incidents have occurred in the past week. 6 were attacks on social medial accounts, 4 were attacks on smart contracts and 1 was a rug-pull.

It is worth noting that the attacks on Zunami Protocol and Exactly Protocol caused a total loss of nearly than US $10 million.

A Reminder for Project Teams: Always test thoroughly. Do smart contract audits before deploying smart contracts on-chain. Be alert to any anomalies happening in the various

social media accounts you manage.

A Reminder for Crypto Users: Be cautious about suspicious links, emails, websites, and projects launched by teams without established reputations.

It is important for everyone in the crypto community to gain understanding and practice sufficient levels of cybersecurity.

To stay updated on notable security incidents in the world of Web3.0, subscribe to our newsletter: https://fairyproof.substack.com/

For a better understanding of all things Web3.0: https://medium.com/@FairyproofT

Looking to strengthen the security of your project or looking for an audit? Contact us at https://www.fairyproof.com/