Weekly Blockchain Security Watch

(June 26 to July 2)

From June 26, 2023 to July 2, 2023, all security incidents that had occurred can be categorized into **Security Hacks and Rug-pulls.**

SECURITY HACKS:

1. **Social Media Accounts Compromised**

From June 26 to July 7, the following social media accounts were compromised and phishing links were sent in these accounts:

The Discord servers of Dackie@Dackie_Official, The Soft DAO@thesoftdao, My Copilot Bae@MyCopilotBae, LightYear.Game@lightyear_game, Oasys@oasys_games, ZigZag Exchange@ZigZagExchange, Entangle Protocol@Entanglefi, Meowcoin@Meowcoin2023, WINR@WINRProtocol, Cilistia@cilistiap2p, Umbrella Network@UmbNetwork, BitKingz@BitKingz, Syntropy@Syntropynet, Radix@radixdlt, ASETPay@ASETPay, Dworfz@Dworfz, Swell@swellnetworkio, Polkadex@polkadex and
The Twitter account of Manta Network@MantaNetwork.

2. **Themis Suffers Exploit**

On June 28, a multi-chain deployed application Themis(@ThemisProtocol) suffered an exploit.

The root cause of the exploit was an inaccurate Balancer LP token price oracle. The attacker exploited this vulnerability to manipulate the LP token price and leveraged a flash loan of around 40,000 WETH from AAVE and two of the Uniswap V3 pools to launch the attack.

The attacker's address:

0xdb73eb484e7dea3785520d750eabef50a9b9ab33 on both Arbitrum/Ethereum.

Crypto assets worth around US $362,000 were exploited in this incident.

3. **Biswap Suffers Exploit**

On July 1, an BNB chain deployed DeFi application Biswap suffered an exploit.

The root cause of the incident was that its implementation lacked parameter verification.

For more details please refer to
https://twitter.com/FairyproofT/status/1675114219933671424?s=20

The attacker's address: 0xe3aeede563bc6a72dc881755cc98dc57fadf30f6 on BNB chain

Crypto assets worth around US $710,251 were exploited in this incident.

4. **Wallet Suffers Phishing Attack**

On July 1, BoredApeYachtClub #8177 #2330 and MutantApeYachtClub #7188 #25145 #20243 #26936 #9188 #15888 #11020 #15454 #417 were stolen and had been sold more than 130 ETHs worth around US $252,000.

The hacker's address: 0x0000553F880fFA3728b290e04E819053A3590000 on Ethereum.

5. **Poly Network Suffers Exploit**

On July 2, a multi-chain deployed cross-chain bridge Poly Network was compromised.

The root cause of this incident was that the cross-chain bridge's private keys were compromised.

Over $42 billion in assets were issued across multiple blockchains including METIS, HECO, BSC, ETH, FTM, OP, POLY, Gnosis and Avalanche.

Crypto assets worth around US $4300,000 were exploited in this incident.

RUG-PULLS:

1. **Chibi Finance Rug-pulls Users**

On June 27, Chibi Finance rug pulled its users for US $1 million, and after that the CHIBI token's price fell by 98%.

CONCLUSION-

6 notable security incidents have occurred in the past week. 1 was a rug-pull and 5 were attacks on smart contracts or wallets.

It is worth noting that Poly Network's exploit was the the second exploit it suffered.

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/