Weekly Blockchain Security Watch

(July 10 to July 16)

From July 10, 2023 to July 16, 2023, all security incidents that had occurred can be categorized into **Security Hacks and Rug-pulls.**

SECURITY HACKS:

1. **Social Media Accounts Compromised**

From July 10 to July 16, the following social media accounts were compromised and phishing links might be sent in these accounts:

holoride@holoride, Overnight.fi@overnight_fi, ReleapProtocol@Releap_IO, UFOGaming@TheUFOtoken, StarProtocol@star_protocol, Superlotl@superlotls, SwapDexBlockchain@SwapdexO, Tapio Finance@TapioFinance and HouseHaeds@HouseHaeds

2. **Arcadia Finance Suffers Exploit**

On July 10, a multi-chain deployed DeFi application Arcadia Finance suffered an exploit.

The root cause is that the application calculated its token price based on the assets stored in the storage and this allowed the hacker to call vaultManagementAction to launch the attack.

The hacker’s address is 0xd3641c912a6a4c30338787e3c464420b561a9467 on OP.

Crypto assets worth around US $ 455K on both Ethereum and Optimism were exploited in this incident.

3. **Libertify Suffers Exploit**

On July 11, a multi-chain deployed DeFi application Libertify suffered an exploit.

The root cause of the exploit is the applicaiton didn’t have re-entrancy protection for its deposit function of the LibertiVault contract. This allowed the attacker to reenter the vulnerable function to steal assets.

The hacker's addresses are 0xfd2D3ffB05aD00E61e3c8D8701cb9036b7A16D02 on ETH and 0xfd2d3ffb05ad00e61e3c8d8701cb9036b7a16d02 on Polygon.

Crypto assets worth around US $ 452,000 were exploited in this incident.

4. **Rodeo Finance Suffers Exploit**

On July 11, an Arbitrum deployed DeFi application Rodeo Finance suffered an exploit.

The root cause is that the application had a vulnerability in its oracle. The hacker exploited this vulnerability to manipulate a token price.

The hacker's address is 0x2f3788F2396127061c46fC07BD0fcb91faAcE328 on Arbitrum

Crypto assets worth around US $ 1.53 million were exploited in this incident.

RUG-PULLS:

1. **Golden Doge King Rug-pulled**

From July 15, an Ethereum deployed token Golden Doge King (0x1093192168a4e3344af3bc01cc19bae02a3fa3d1 on ETH) was confirmed to be a rug-pull.

Around 22ETHs worth around US $42,000 were exploited in this incident.

CONCLUSION-

13 notable security incidents have occurred in the past week. 9 were attacked on social medial accounts, 3 were attacks on smart contracts and 1 was a rug-pull.

It is worth noting that attack on Rodeo Finance caused a loss of US $ 1.53 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/