Top 10 Web3 Hacks of 2023: Expert Insights by Salus

SINGAPORE, January 19, 2024 /EINPresswire.com/ -- 2023 marked a significant turning point, witnessing reported losses surpassing $1.7 billion across approximately 453 incidents. Salus, at the forefront as an expert team, meticulously analyzed this landscape, identifying vulnerabilities that led to substantial losses. The top 10 hacks, constituting nearly 70% of the total losses, reveal a common thread – access control issues, particularly private key thefts.

2023 Top 10 Hacks Timeline

Top 10 Hacks of 2023

1. Mixin Network: Clouds Part, Assets Vanish
Mixin Network experienced a significant breach, resulting in a $200 million loss. Attackers targeted the database of Mixin Network's cloud service provider, raising concerns about the security of cloud service providers.

2. Euler Finance: Vulnerability in DeFi Protocol
Euler Finance suffered a substantial loss of $197 million due to a vulnerability in the donateToReserves function. The incident underscored the importance of rigorous smart contract auditing and risk assessment in decentralized finance (DeFi) protocols.

3. Multichain: Keys Lost, Chains Shattered
Multichain experienced an abnormal movement of lockup assets to an unknown address, raising questions about the security practices of Multichain. The incident highlighted potential risks

associated with administrator keys and internal security practices.

4. Poloniex: Lazarus Strikes, Keys Compromised
Poloniex cryptocurrency exchange fell victim to a hack orchestrated by the Lazarus Group, resulting in a $126 million loss. The incident exemplified the classic vulnerability of compromised hot wallets.

5. BonqDAO: Oracle's Gamble, Protocol's Plunge
The Polygon-based lending and stablecoin protocol, BonqDAO, suffered a two-stage attack involving oracle manipulation, resulting in a $120 million loss. The incident highlighted the risks associated with oracle vulnerabilities and their potential impact on DeFi platforms.

6. Atomic Wallet: North Wind Blows, Lawsuit Echoes
Atomic Wallet experienced a loss of over $100 million as addresses were drained through a three-step system. The North Korean Lazarus Group was identified as the perpetrator, leading to legal consequences and emphasizing the responsibility of platforms to address known vulnerabilities.

7. HECO Bridge, HTX: Bridges Burn, Wallets Drained
$86.6 million was lost from HECO Chain's Ethereum bridge and $12.5 million from hot wallets belonging to HTX (formerly Huobi). The HECO Bridge funds were drained via a compromised operator account, highlighting the need for secure infrastructure in decentralized bridges.

8. Curve, Vyper: Bug's Ballet, Pool's Lament
Curve, relying on Vyper, faced a $69.3 million loss due to a 0-day compiler bug. The incident highlighted the potential risks associated with language-specific vulnerabilities in smart contracts.

9. AlphaPo: Lazarus' Silent Heist
AlphaPo, a crypto payments processor for gambling platforms, lost $60 million across ETH, TRON, and BTC. The attack, likely orchestrated by Lazarus, raised awareness about the evolving tactics of sophisticated hacking groups.

10. CoinEx: Keys Leaked, Wallets Emptied
CoinEx suffered a loss of $54.3 million due to a compromised hot wallet private key. Anomalous withdrawals from several hot wallet addresses led to the incident, highlighting the vulnerability of hot wallet private keys.

Expert Insights: Deciphering Common Vulnerabilities

The top 10 hacks of 2023, constituting nearly 70% of total losses, underscore a common vulnerability – access control issues, particularly private key thefts. These breaches predominantly occurred in the second half of the year, with November witnessing three major

attacks. The Lazarus Group played a significant role in multiple breaches, draining funds from compromised hot wallets.

Strengthening Your Web3 Security

In the wake of these challenges, Salus stands ready to fortify your project's security. With expertise in smart contract audits, Web3 penetration testing, and cutting-edge ZK solutions, Salus is committed to elevating the security standards of your platform. Trust Salus to navigate the complexities of the Web3 landscape and safeguard your digital assets.

Source: https://salusec.io/blog/web3-security-landscape-report
Learn more: https://linktr.ee/salus_security

Shawn
Salus
email us here
Visit us on social media:
Twitter
LinkedIn
