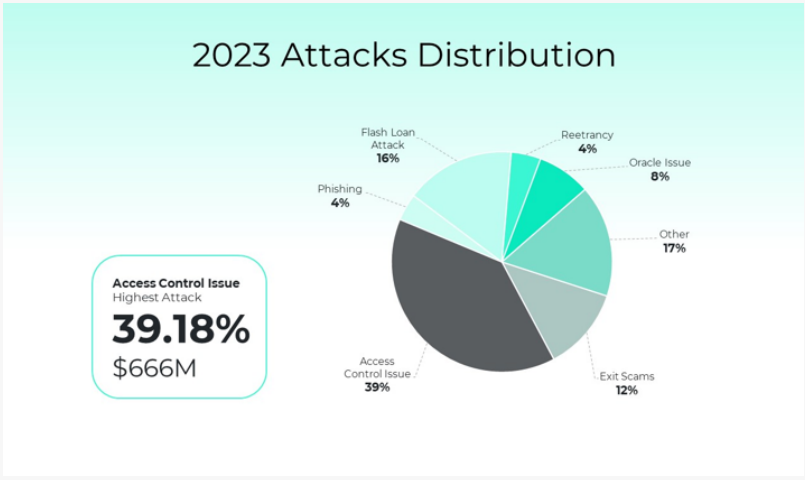
Safeguarding Against Web3 Vulnerabilities: A Salus Guide to the $666 Million Access Control Challenge

SINGAPORE, January 19, 2024 /EINPresswire.com/ -- The digital landscape underwent a significant transformation, revealing a striking $1.7 billion in losses across 453 reported incidents in 2023. This underscores the ever-present and evolving nature of cyber threats. Salus, a leader in web3 security, conducted a thorough analysis to unravel the intricacies of these challenges.

2023 Top 10 Hacks Timeline



2023 Attacks Distribution

Decoding Top 10 Hacks of 2023 with Salus

The year 2023 saw a convergence of significant breaches, with the top 10 hacks constituting nearly 70% of total losses. Salus's analysis pinpointed a common vulnerability – access control issues, particularly private key thefts. The Lazarus Group played a significant role in multiple breaches, draining funds from compromised hot wallets.

Web3 Vulnerabilities in 2023:

Within the core of the report, Salus uncovered critical vulnerabilities in the Web3 domain, showcasing a diverse array of threats. Exit scams constituted 12.24% of attacks, resulting in a $208 million loss, emphasizing the need for vigilant research and investment diversification. Access control issues took center stage, representing 39.18% of attacks and causing losses totaling $666 million. Phishing incidents, accounting for 3.98% of attacks. Furthermore, flash loan attacks, reentrancy vulnerabilities, and oracle issues collectively contributed to substantial

losses, showcasing the multifaceted nature of threats in the Web3 landscape.

Preventing Web3 Vulnerabilities: Salus's Strategic Focus

Exit Scams: Building Trust Through Due Diligence

 Prioritize thorough research on projects and teams, ensuring a solid track record. Embrace projects with transparent security assessments from reputable firms, enhancing trust and resilience against exit scams.

Access Control Issues: Strengthening Digital Gates

 Implement robust authentication and authorization mechanisms, adhering to the principle of least privilege. Regularly update access permissions, conduct regular security audits and establish comprehensive monitoring systems to detect and respond to any suspicious activities promptly.

Phishing: Empowering Users with Education

 Conduct Web3 penetration testing to identify vulnerabilities in the system that phishers could exploit. Prioritize user education, advocate for hardware wallets and multi-factor authentication (MFA), and employ email verification and domain monitoring to combat phishing attacks.

Flash Loan Attacks: Adding Hurdles for Attackers

 Mitigate flash loan risks by implementing restrictions like minimum borrowing amounts and time limits. Conduct regular security audits and introduce fees for flash loan usage to raise the cost for attackers, acting as a deterrent against malicious exploits.

Reentrancy: Thwarting Persistent Smart Contract Risks

 Accounting for 4.35% of attacks, reentrancy vulnerabilities caused a loss of $74 million. Adhering to the Check-Effect-Interaction model and implementing comprehensive reentry protection are crucial safeguards.

Oracle Issues: Enhancing Market Resilience

 Avoid using markets with shallow liquidity for price predictions. Assess token liquidity before considering specific price oracle plans. Increase the attacker's manipulation cost through Time-Weighted Average Price (TWAP) to make exploitation less attractive.

Other Vulnerabilities: A Holistic Security Approach

 Representing 16.47% of attacks, various vulnerabilities caused a loss of $280 million. From Mixin's database breach to web2 vulnerabilities, this category showcased diverse security challenges in the Web3 space

Salus - Your Shield Against Vulnerabilities

As we navigate the challenges of Web3 in 2023, Salus's commitment to proactive security shines

through. By understanding vulnerabilities and implementing preventive measures, users and stakeholders can contribute to fortifying the Web3 ecosystem, ensuring a resilient and secure digital future.

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
