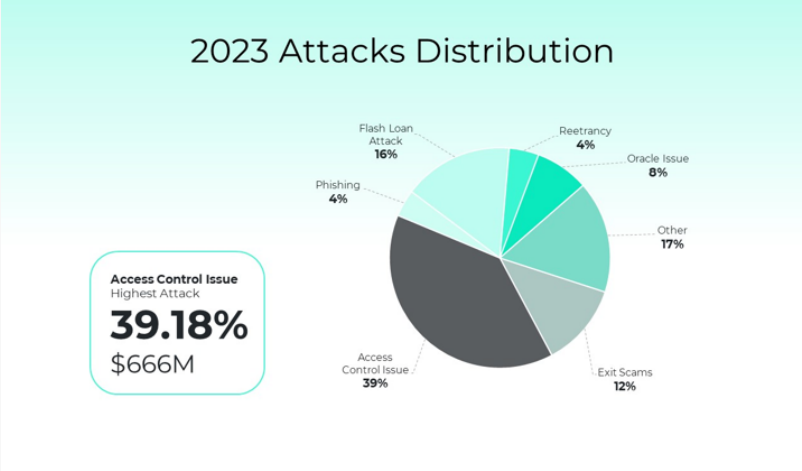
Web3 Security Risks in 2023: Expert Insights

SINGAPORE, January 15, 2024 /EINPresswire.com/ -- In the ever-evolving landscape of Web3, the year 2023 marked a pivotal moment in the realms of innovation and adversity. As the guardians of web3 security, Salus, a distinguished research-driven security company, played a crucial role in dissecting the intricate patterns of cyber threats that unfolded throughout the year.



2023 Attacks Distribution

2023 Monthly Exploit Losses

Introduction: Unravelling Web3 Challenges

The digital frontier witnessed a dramatic shift in the balance between resilience and vulnerability. In the wake of 2023, the Web3 industry bore witness to a staggering $1.7 billion in losses across approximately 453 reported incidents, an alarming testament to the persistent and evolving nature of cyber threats.
Key Trends and High-Profile Exploits:

Salus's meticulous examination of the 2023 Web3 Security Landscape Report highlighted a stark contrast in trends. While overall losses showed a decline, the industry resonated with high-profile exploits. Noteworthy breaches, such as Mixin Network's $200 million loss in September, Euler Finance's $197 million setback in March, and Multichain's $126.36 million incident in July, underscored persistent threats targeting bridges and decentralized finance (DeFi) protocols.

Web3 Vulnerabilities: A Deep Dive

1. Exit Scams: The Illusion of Returns:
Accounting for 12.24% of attacks, exit scams resulted in a loss of $208 million. These scams,

promising high returns, underscore the importance of vigilant research and diversified investments.

2. Access Control Issues: Gateways to Losses:
Representing 39.18% of attacks, access control issues caused losses totalling $666 million. Robust authentication mechanisms and ongoing security training are crucial countermeasures.

3. Phishing: Unveiling Front-End Vulnerabilities:
Constituting 3.98% of attacks, phishing incidents highlighted front-end vulnerabilities. Web3 penetration testing, user education, and hardware wallets are essential safeguards.

4. Flash Loan Attacks: Precision in Exploitation:
Contributing to 16.12% of attacks, flash loan incidents resulted in a loss of $274 million. Implementing restrictions, introducing fees, and conducting regular security audits act as deterrents against malicious exploits.

5. Reentrancy: Mitigating 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.

6. Oracle Issues: Manipulating the Unseen:
Constituting 7.88% of attacks, oracle issues led to a loss of $134 million. Safeguards include avoiding markets with shallow liquidity, assessing token liquidity, and increasing the attacker's manipulation cost through Time-Weighted Average Price (TWAP).

7. Other Vulnerabilities: A Diverse Spectrum:
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.

Tightening Web3 Security with Salus: Expert Solutions for a Safer Future

As a security sentinel, Salus actively participated in crafting solutions to navigate these challenges. From providing in-depth insights into vulnerabilities to recommending actionable safety measures, demonstrating a commitment to securing the Web3 future.

In conclusion, the concentration of losses in the top 10 hacks emphasizes the need for heightened security measures. Salus, with its expertise in smart contract audits and web3 penetration testing, stands ready to guide users and stakeholders towards platforms that prioritize both functionality and security. As we traverse the ever-evolving Web3 landscape, Salus serves as a beacon of trust and reliability, a testament to its unwavering commitment to the security industry.

Learn more: https://linktr.ee/salus_security

Shawn
Salus
pr@salusec.io
Visit us on social media:
Twitter
LinkedIn
