Vol. 2 - No. 2
March 2025 E-ISSN: 2584-0657

Wazrix Security Breach

Sridhar M[1], Arun S[2], Harini U[3], Jayaraj R[4], Rithika P[5]
[1,2,3,4] *Cyber Security, Sree Sakthi Engineering College, Coimbatore, Tamil Nadu, India*
[5] *Assistant Professor, Department of Emerging Technologies*
Sree Sakthi Engineering College, Coimbatore, Tamil Nadu, India
***DOI**: https://doi.org/10.5281/zenodo.15641594*

Abstract

The Wazirx cryptocurrency exchange, one of India's largest platforms, experienced a significant security breach in July 2024, resulting in the unauthorized transfer of over $230 million in digital assets. The attack exploited vulnerabilities in a multisignature (multisig) Ethereum wallet managed in collaboration with Liminal, a digital asset custody provider. Attackers manipulated discrepancies between the transaction data displayed on Liminal's interface and the actual transaction content, gaining unauthorized control over the wallet. Preliminary investigations suggest potential involvement of the Lazarus Group, a North Korean state-sponsored cybercriminal organization known for targeting cryptocurrency exchanges.

Wazirx responded swiftly by informing relevant authorities, including the Financial Intelligence Unit (FIU) and CERT-In, while collaborating withover500 exchanges globally to block malicious addresses. A bounty program offering up to $10,000 in USDT was also launched to incentivize actionable intelligence for recovering stolen funds. This incident highlights critical vulnerabilities in multisig wallet configurations and emphasizes the need for continuous security assessments and proactive threat mitigation.

This research examines the vulnerabilities in decentralized finance (DeFi) platforms, focusing on the exploitation of multisig wallets and analyzing transaction logs to identify the role of manipulated transaction payloads and discrepancies in wallet interface data. The study explores the involvement of advanced threat actors such as the Lazarus Group and highlights gaps in existing DeFi security mechanisms. It proposes enhanced payload validation, improved cryptographic safeguards, and real-time anomaly detection systems to fortify DeFi platforms against evolving threats.

INTRODUCTION

WazirX is a leading cryptocurrency exchange in India that provides a platform for selling, buying, and trading cryptocurrencies such as Bitcoin, Ethereum, and Dogecoin. WazirX security breach on July 18, 2024, was a major cyber attack on one of the cryptocurrency exchange's multisig wallets. The breach led to the theft of more than $230 million in digital assets, which represented close to half of Wazirxs reserves.

Mechanism of the Breach

The attackers manipulated a discrepancy between the data displayed on Liminal's interface (a digital asset custody service) and the actual transaction contents. This allowed them to replace the payload and gain unauthorized control over the wallet

Impact

The breach affected nearly half of WazirX's reserves, leading to a temporary halt in deposits, withdrawals, and trading

METHODOLOGY TO SECURE WAZRIX

Multi-Signature Wallets

A multisig wallet requires multiple private keys to authorize a transaction, enhancing security by distributing control among several parties. For example, a 2-of-3 multisig wallet requires any two of the three private keys to approve a transaction.

Multisim Wallet Structure in Wazir

Signatories: The impacted multisig wallet of WazirX had six signatories—five under the control of WazirX and one under Liminal, a digital asset custody provider.

Signing Process: Three signatures from WazirX signers and one additional signature from Liminal were needed for transactions. This multi-layered structure was intended to prevent any one partyfrom being able to authorize a transaction unilaterally.

Liminal's Role: Liminal was the ultimate safeguard of defense, checking the legitimacy of transactions prior to authenticating them with a signature. They had extra protection such as firewalls and destination whitelisting in their infrastructure.

Two Factor Authentication (2FA)

WazirX two-factor authentication security breach operated in the following manner:

Extra Verification: 2FA mandated users to furnish a second method of authentication, like an OTP through SMS, email, or authenticator software like Google Authenticator or Authy.

Time-Sensitive Codes: The authenticator applications produced time- limited codes which had an expiry time of 30 seconds for dynamic security.

Recovery Mechanism: Recovery codes could be used or recovery and restoration of the 2FA can be requested using recovery codes or WazirX support team.

Prevention from Phishing: Access to key systems was via trusted links to prevent phishing attacks.

Impact during Breach: Although 2FA protected individual accounts, the breach took advantage of weaknesses in other aspects, including the multisig wallet design

Hardward Wallet

Hardware wallets are specialized physical devices for storing cryptocurrency private keys offline. Their design provides protection against online attacks such as hacking or malware.

Fundamental Functions

Offline Private Key 30 Storage: Hardware wallets store private keys in a secluded, secure environment.

Transaction Signing: Physical authentication (e.g., button press) is needed to sign a transaction, making it virtually impossible to access without authorization.

Multisig Wallet Integration: WazirX utilized hardware wallets as part of its multisignature implementation, where multiple authorized signers had to authorize transactions.

Phishing Resistance: By storing private keys offline, such wallets reduce the risk ofexposure to phishing or malware attacks.

Bounty Programs

Bounty programs are programs that are implemented to improve security and encourage collaboration with ethical hackers and security researchers. In WazirX, such programs are intended to enhance the security measures of the platform and remedy vulnerabilities.

Track & Freeze Bounty: Volunteers were encouraged to share actionable intel to track and freeze stolen money. Rewards up to $10,000 value in USDT were given for successful submissions2.

White Hat Recovery Bounty: White-hat hackers and cybersecurity professionals were in centivized to help recover stolen money. A reward of 10% of the recovered money (up to $23 million) was provided as an incentive2.

Community Collaboration: The initiative invited international experts, including blockchain forensic professionals, to share their expertise and experience3.

Timeframe: The bounty program was at first available for three months but was extendable on a recovery-dependent basis3.

Transparency and Confidentiality: Submitter shad to keep the information confidential and submit detailed reports, including addresses, transactions, and methods.

Regular security audits are systematic examinations of applications, systems, or databases to ensure reliability and identify vulnerabilities.

Scope of Audits: WazirX conducted audits on its systems, including blockchain code and smart contracts, to detect bugs or defects.

Compliance Checks: Audits ensured adherence to regulatory standards, such as the Common Criteria for IT Security Evaluation.

Third-Party Reviews: Peer reviews by outside professionals were done to ensure the security measures.

Proactive Measures: WazirX actively flagged accounts with dubious activities and reported information to law enforcement authorities.

ERC 20 Transaction

An ERC20 transaction is the exchange of tokens developed based on the ERC20 standard within the Ethereum blockchain. The ERC20 standard dictates a predefined set of rules and functions that developers have to adhere to when they develop tokens for compatibility with wallets, exchanges, and decentralized applications (dApps).

Smart Contract Exploitation: The exploit took advantage of vulnerabilities in the smart contract managing the wallet, stressing the need for strict audits.

Phishing and Social Engineering: Although not directly at tested, these attacks typically use phishing mechanisms to steal signatories' credentials.

PRILIMINARY ANALYSIS

Scenario 1

All three WazirX signers were directly sent malicious transactions by Liminal through possible breach of the Liminal infrastructure. This is a possible scenario that is evidenced by:

- No new connection request was made to the hardware wallets
- The request was made from a whitelisted address as viewed by the WazirX signers on the Liminal interface.
- All signers viewed the anticipated token name (USDT and GALA) and destination address on the Liminal interface and also received email notifications

Scenario 2

All three WazirX signers were compromised by malware on three devices by some means by the attackers. Though we haven't seen any initial indication of malware, we did begin the forensic test and shall let you know what we found in the next few days. As an interesting note, if this were going to be a feasible scenario, the attacker would also have had to penetrate into Liminal's infrastructure and firewall in order to gain access to the fourth and last signature so they could then run and submit a transaction onto the blockchain.

Since our initial investigation indicates no trace of tampering or malicious malware on our network, we presently suspect Scenario 1 as the most probable cause of this attack.

MISSING SECURITY MEASURES

Discrepancy in Data Verification

Discrepancy in data verification is a term used to describe inconsistencies or discrepancies between data that is being shown on an interface and the real transaction or payload contents. It can arise from data processing, transmission, or display errors that cause system vulnerabilities in the case of systems that are dependent upon proper data verification.

Attackers took advantage of a discrepancy between data presented on Liminal's interface and the true transaction pay load. This enabled them to manipulate the transaction information and take unauthorized control of the multisig wallet

Implement Strong Data Integrity Checks

- Make sure data presented on interfaces is the same as the actual transaction contents.
- Use cryptographich as hing to verify the integrity of transaction payloads.

Enhance Multisig Wallet Security

- Introduce additional layers of authentication for multisig wallets.
- Regularly audit wallet infrastructure to detect and correct vulnerabilities.

Deploy Real-Time Monitoring Systems

- Utilize AI-based tools to monitor transactions and identify anomalies in real-time.
- Flag and suspend suspicious activity right away.

Perform Regular Security Audits

- Run regular vulnerability scans and penetration testing.
- Partner with security experts to determine where vulnerabilities may reside.

Train Employees and Users

- Train employees on cybersecurity best practices to minimize human errors.
- Inform users about potentials cams and secure transaction methods.

Develop a Comprehensive Incident Response Plan

- Develop procedures for immediate response in the event of a breach.
- Work with law enforcement and cybersecurity professionals for recovery purposes.

Utilize Blockchain-Specific Solutions

Use blockchain-based data integrity verification solutions to provide tamper-proof transactions

Multisig Wallet Vulnerabilities

A multisig wallet (also known as a multi-signature wallet) is a digital wallet for cryptocurrency that demands more than one private key (signatures) to approve a transaction, providing greater security than single-signature wallets. Vulnerabilities happen when there are flaws in the implementation, handling, or verification of the multisig infrastructure, making it susceptible to exploitation by malicious users.

The multisig wallet was attacked since attackers leveraged vulnerabilities within the custody framework and approval transactions. Precisely, because there were insufficient strong protections in place, they were able to manipulate the course of transactions as well as dodge the requirement of legitimate multiple approvals.

Secure the Multisig Implementation

- Ensure that the cryptographic protocols used for generating and verifying signatures are up to date and free of known vulnerabilities.
- Use well-audited, open-source frameworks to eliminate hidden flaws in proprietary systems.

Enforce Strict Key Management Practices

- Distribute private keys across multiple trusted parties, devices, or locations to avoid a single point of failure.
- Use hardware security modules (HSMs) or cold wallets for secure key storage.

Verify the Transaction Payload at Every Step

- Implement verification mechanisms at multiple stages during a transaction’s lifecycle to ensure its integrity.
- Display the exact transaction details (e.g., amount, recipient address) to each signer for validation before authorization.

Deploy Real-Time Monitoring and Alerts

- Implement AI or machine learning-based monitoring software to identify unauthorized or suspicious patterns of transactions.
- Implement alerts for any discrepancies in the multisig authorization process.

Establish Clear Access Controls and Permissions

- Restrict access to the multisig wallet interface to only authorized individuals.
- Apply role-based access control to establish who is permitted to sign transactions and under which circumstances.

Execute Employee and Partner Training Programs

- Educate staff on multisig wallet functionality and the need to follow security procedures.
- Roll out training to partners or third-party custodians to provide system-wide security.

KEY INSIGHT: THE EVOLVING LANDSCAPE OF MULTISIG ETHEREUM WALLET SECURITY

As we research this incident, we've learned some important lessons about the intricacies of securing multisig Ethereum wallets. We'd like to pass along our findings that can help improve security practices throughout the entire crypto ecosystem:

The crypto space still has a major security problem on its hands, with multisig wallets and intricate smart contract interactions being focal points for concern. When processing ERC20 transactions, hardware wallets usually don't show the token or destination address. Blind signing is when a hardware wallet doesn't completely reveal the information of the transaction you are signing off on, including the destination address and the details of the tokens that are being moved. This "blind signing" is a recognized limitation in most configurations where signers have to trust the information displayed on their custody provider's interface, trusting implicitly what they see on the screen. If an infrastructure of a custody provider is hacked, there is a theoretical risk that information displayed on the screen could be tampered with, even with strong security controls in place.

This weakness is not specific to WazirX – it is a recurring problem in Ethereum multisig transactions. The Ledger supply chain attack earlier this month (December 14, 2023) raised this problem to the surface, prompting Ledger to announce plans to turn off blind signing for EVM dApps by default. Subsequently, Ledger also made plans to turn off blind signing for EVM dApps during December 2023.

On our part, to reduce risks related to blind signing, we adhered to best practices suggested by hardware wallet vendors (Ledger), such as:

Checking the URL of the website we're dealing with.

Making sure we're dealing with a trusted platform. Keeping private keys in hardware wallets, offline. Using multi-factor authentication and geographically dispersed signers.

Using book marked links to avoid phishing.

The crypto ecosystem has always excelled through community collaboration and cooperation. We intend to share this knowledge to feed into the global knowledge that has the potential to make our industry safer for everyone. Together, we can work towards a secure environment for all crypto users.

It's about protecting the future of decentralized finance and millions of users' trust globally.

CONCLUSION

Serious vulnerabilities in Multi signature wallet security were revealed by the Wazir hack in July 2024, mostly due to UI-payload discrepancies and poor validation processes. The research highlights the importance of having strict access controls, real- time anomaly detection, and secure verification of transactions in cryptocurrency exchanges. To minimize damage and regain customer trust, the hack also stresses the importance of international collaboration and an immediate open response. Decentralized finance (DeFi) platforms can make themselves more resilient to evolving cyber threats and ensure secure digital asset transfers in the future by eliminating these vulnerabilities through better user awareness, improved cryptographic protections, and regular security auditing.

REFERENCES

[1] Venugopal, Sahana (3September 2024). "WazirX Cyberattack: What is WazirX's legal status after a $230 million wallet hack?". The Hindu.

[2] "WazirX cryptocurrency exchange suspends withdrawals following security breach". The Indian Express. 2024-07-18. Retrieved 2024-07-31

[3] Shukla, Siddharth (2024-07-18). "WazirX Suspends Crypto, Rupee Withdrawals After Wallet Breach". Bloomberg.com. Retrieved 2024-07-31

[4] Anand, Vijay (2024-07-29). "North Korean Lazarus Group behind $235 million WazirX crypto breach - CNBC TV18". CNBCTV18. Retrieved 2024-07-31

[5] "WazirX Hit by $235 Million Hack, Suspects Lazarus Group". Financial Times. 2024-07-18. Retrieved 2024-07-31.

[6] Kumar, Abhinav (2024-07-20). "WazirX Withdrawals Halted After Major Breach". The Economic Times. Retrieved 2024-07-31.

[7] "WazirX to Socialize $230 Million Security Breach Loss Among Customers". Business Line. 2024-07-18. Retrieved 2024-07-31.

[8] Gupta, Pooja (2024-07-19). "WazirX Crypto Hack: What Went Wrong?". Tech Crunch India. Retrieved 2024-07-31.

[9] "Cryptocurrency Exchange WazirX Hit by $230 Million Security Breach". Reuters. 2024-07-19. Retrieved 2024-07-31.

[10] "Analysis: WazirX Hack and Its Implications for Indian Crypto Regulations". The Wall Street Journal. 2024-08-01. Retrieved 2024-08-02.

[11] Patel, Harsh (2024-07-21). "Crypto Crime: WazirX Hack Linked to Lazarus Group". The Verge. Retrieved 2024-07-31.

[12] "Security Failures Behind WazirX's $230 Million Loss". Coin Desk. 2024-07-22. Retrieved 2024-07-31.

[13] "North Korea’s Lazarus Group Behind WazirX Breach, Says Report". India Today. 2024-07-23. Retrieved 2024-07-31.

[14] "Understanding the WazirX Hack and Cryptocurrency Security". Cybersecurity Journal. 2024-08-02. Retrieved 2024-08-03.

[15] "Blockchain Forensics: Tracing Stolen Funds in the WazirX Hack". Silicon ANGLE. 2024-07-20. Retrieved 2024-07-31.