



DISPUTES AND INVESTIGATIONS

2024 10 17

SECURITY CONCERNS AT WORMHOLE PORTAL: 4 KEY TAKEAWAYS



Calvin K. Koo

Partner
calvin.koo@kobrekim.com



Evelyn Baltodano Sheehan

Partner
evelyn.sheehan@kobrekim.com



Jake Calvert

Partner
jake.calvert@kobrekim.com



Jonathan D. Cogan

Partner
jonathan.cogan@kobrekim.com



Kiran Unni

Partner
kiran.unni@kobrekim.co.uk



Nicholas Surmacz

Partner
nicholas.surmacz@kobrekim.co.uk



Peter Tyers-Smith

Partner
peter.tyers-smith@kobrekim.ky

On October 17, 2024, Wormhole Portal, a leading Web3 gateway, announced a security incident involving the theft of 120,000 wETH from its platform. The incident, which occurred on October 16, 2024, involved a vulnerability in the platform's smart contracts that allowed an attacker to drain funds from the platform's wallet. The attacker, identified as Tao Mao Shan Limited, used a technique known as "TMSL" (Transaction Manipulation and Signature Logic) to execute the theft. The incident highlights the importance of robust security measures in the Web3 ecosystem and the potential risks associated with smart contract vulnerabilities.

On October 17, 2024, Wormhole Portal, a leading Web3 gateway, announced a security incident involving the theft of 120,000 wETH from its platform. The incident, which occurred on October 16, 2024, involved a vulnerability in the platform's smart contracts that allowed an attacker to drain funds from the platform's wallet.

Key Takeaway 3.2: TMSL

On October 17, 2024, Wormhole Portal, a leading Web3 gateway, announced a security incident involving the theft of 120,000 wETH from its platform. The incident, which occurred on October 16, 2024, involved a vulnerability in the platform's smart contracts that allowed an attacker to drain funds from the platform's wallet. The attacker, identified as Tao Mao Shan Limited, used a technique known as "TMSL" (Transaction Manipulation and Signature Logic) to execute the theft. The incident highlights the importance of robust security measures in the Web3 ecosystem and the potential risks associated with smart contract vulnerabilities.

TMSL is a technique used by attackers to manipulate transactions and execute unauthorized actions on a blockchain network. In this case, the attacker used TMSL to execute a transaction that drained funds from the platform's wallet. The incident highlights the importance of robust security measures in the Web3 ecosystem and the potential risks associated with smart contract vulnerabilities.

On October 17, 2024, Wormhole Portal, a leading Web3 gateway, announced a security incident involving the theft of 120,000 wETH from its platform. The incident, which occurred on October 16, 2024, involved a vulnerability in the platform's smart contracts that allowed an attacker to drain funds from the platform's wallet. The attacker, identified as Tao Mao Shan Limited, used a technique known as "TMSL" (Transaction Manipulation and Signature Logic) to execute the theft. The incident highlights the importance of robust security measures in the Web3 ecosystem and the potential risks associated with smart contract vulnerabilities.

On October 17, 2024, Wormhole Portal, a leading Web3 gateway, announced a security incident involving the theft of 120,000 wETH from its platform. The incident, which occurred on October 16, 2024, involved a vulnerability in the platform's smart contracts that allowed an attacker to drain funds from the platform's wallet. The attacker, identified as Tao Mao Shan Limited, used a technique known as "TMSL" (Transaction Manipulation and Signature Logic) to execute the theft. The incident highlights the importance of robust security measures in the Web3 ecosystem and the potential risks associated with smart contract vulnerabilities.

On October 17, 2024, Wormhole Portal, a leading Web3 gateway, announced a security incident involving the theft of 120,000 wETH from its platform. The incident, which occurred on October 16, 2024, involved a vulnerability in the platform's smart contracts that allowed an attacker to drain funds from the platform's wallet.

On October 17, 2024, Wormhole Portal, a leading Web3 gateway, announced a security incident involving the theft of 120,000 wETH from its platform. The incident, which occurred on October 16, 2024, involved a vulnerability in the platform's smart contracts that allowed an attacker to drain funds from the platform's wallet. The attacker, identified as Tao Mao Shan Limited, used a technique known as "TMSL" (Transaction Manipulation and Signature Logic) to execute the theft. The incident highlights the importance of robust security measures in the Web3 ecosystem and the potential risks associated with smart contract vulnerabilities.

On October 17, 2024, Wormhole Portal, a leading Web3 gateway, announced a security incident involving the theft of 120,000 wETH from its platform. The incident, which occurred on October 16, 2024, involved a vulnerability in the platform's smart contracts that allowed an attacker to drain funds from the platform's wallet.

This content provides information on legal issues and developments of interest to our clients and friends and should not be construed as legal advice on any matter, specific facts or circumstances. The distribution of our content is not intended to create, and receipt of it does not constitute, an attorney-client relationship.

