



DISPUTES AND INVESTIGATIONS

2024 10 17

SECURITY CONCERNS AT WORMHOLE PORTAL: 4 KEY TAKEAWAYS



Calvin K. Koo

Partner
calvin.koo@kobrekim.com



Evelyn B. Sheehan

Partner
evelyn.sheehan@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



Steven W. Perlstein

Partner
steven.perlstein@kobrekim.com

On October 17, 2024, Wormhole Portal, a leading Web3 infrastructure provider, announced a security incident involving the theft of 120,000 wETH from its platform. This incident has raised significant concerns about the security of Web3 infrastructure and the potential for large-scale thefts. In this article, we discuss the key takeaways from this incident and the implications for the Web3 ecosystem.

The incident involved the theft of 120,000 wETH from Wormhole Portal, a leading Web3 infrastructure provider. The theft was attributed to a vulnerability in the platform's security protocol, which allowed attackers to bypass security measures and steal funds. This incident highlights the need for robust security protocols in Web3 infrastructure.

Key Takeaway 3.2: Security Protocols

Wormhole Portal, a leading Web3 infrastructure provider, announced a security incident involving the theft of 120,000 wETH from its platform. The incident was attributed to a vulnerability in the platform's security protocol, which allowed attackers to bypass security measures and steal funds. This incident highlights the need for robust security protocols in Web3 infrastructure.

TMSL, a leading Web3 infrastructure provider, announced a security incident involving the theft of 120,000 wETH from its platform. The incident was attributed to a vulnerability in the platform's security protocol, which allowed attackers to bypass security measures and steal funds. This incident highlights the need for robust security protocols in Web3 infrastructure.

TMSL, a leading Web3 infrastructure provider, announced a security incident involving the theft of 120,000 wETH from its platform. The incident was attributed to a vulnerability in the platform's security protocol, which allowed attackers to bypass security measures and steal funds. This incident highlights the need for robust security protocols in Web3 infrastructure.

TMSL, a leading Web3 infrastructure provider, announced a security incident involving the theft of 120,000 wETH from its platform. The incident was attributed to a vulnerability in the platform's security protocol, which allowed attackers to bypass security measures and steal funds. This incident highlights the need for robust security protocols in Web3 infrastructure.

TMSL, a leading Web3 infrastructure provider, announced a security incident involving the theft of 120,000 wETH from its platform. The incident was attributed to a vulnerability in the platform's security protocol, which allowed attackers to bypass security measures and steal funds. This incident highlights the need for robust security protocols in Web3 infrastructure.

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.

© 2025 Kobre & Kim LLP. All Rights Reserved. Prior Results DO NOT Guarantee A Similar Outcome.

