hathor

ENHANCING SECURITY FOR THE HATHOR WALLETS AND FULL NODE

THE WALLETS

We have taken significant steps to strengthen the security of the Hathor wallets by implementing LavaMoat, a powerful security tool designed for JavaScript applications. This document outlines how LavaMoat improves wallet security and protects users from potential threats.

PROTECTING AGAINST SUPPLY CHAIN ATTACKS

LavaMoat acts as a shield against a type of threat called supply chain attacks. These attacks occur when malicious code sneaks into an application through seemingly harmless third-party software packages. This just happened with DogWifTools, and with Solana's library last year.

Here's how LavaMoat helps:

- It creates a protective bubble around each software package used in the wallet.
- This bubble limits what each package can do, reducing the potential damage if one becomes compromised.
- It prevents harmful code from tampering with core JavaScript functions.
- LavaMoat controls which parts of the system each package can access, adding an extra layer of protection.

ADDRESSING SPECIFIC VULNERABILITIES

LavaMoat is particularly effective against certain types of attacks:

- It guards against incidents similar to past wallet hacks where malicious code was inserted through trusted software packages.
- By isolating packages, it stops unauthorized code from running freely within the wallet.
- LavaMoat carefully manages which parts of the system each package can interact with, preventing potential misuse.

ADDITIONAL SECURITY MEASURES

LavaMoat introduces several key security features:

- It uses special containers to run code, making it harder for malicious software to operate.
- A security policy is created for the wallet, specifying exactly what each part of the software is allowed to do.

- LavaMoat can extend its protection to all areas of the wallet application, closing off potential weak spots.

By considering these security measures, Hathor aims to significantly reduce the risk of attacks on our wallets. This approach helps protect user funds and information by creating multiple layers of defense against potential security threats in the software used to build the wallets.

FULL NODE IMPROVEMENTS

Hathor's full node implements robust security measures for peer management to protect against various attack vectors. The node employs a sophisticated approach to handling entry points, which are the initial connections a node makes to join the network.

To prevent entrypoint poisoning and maintain network integrity, Hathor's full node uses a shuffling strategy for entry points that doesn't favor any single peer, especially those attempting to flood the network with potentially malicious entry points. The node also maintains separate lists for entry points received from different peers and imposes limits on these lists to prevent resource exhaustion attacks.

Connection management is another critical aspect of Hathor's full node security. The node utilizes distinct connection pools for different purposes, such as outgoing connections, incoming connections, and potentially separate pools for health checks and peer verification. Each pool has its own limit to ensure balanced resource allocation and prevent any single type of connection from overwhelming the node.

To further enhance security and privacy, Hathor's full node is designed to never broadcast all known peers. This approach likely involves maintaining a separate pool of nodes that are not broadcast to anyone, reducing the risk of targeted attacks on specific nodes. Additionally, the node implements timeouts for various states and connection types, ensuring that no connection can indefinitely consume resources.

These measures collectively contribute to a more resilient and secure peer-to-peer network for Hathor, protecting against common attack vectors such as eclipse attacks, Sybil attacks, and denial-of-service attempts.

If you plan on integrating with Hathor, you should check out our integration best practices blog post.