**CERT Outreach Brief: Bitcoin Witness Forgery Exploit ("Bitcoin Kidnapping")**

**Document Classification**: CONFIDENTIAL / ETHICAL DISCLOSURE

**Prepared by**: [Red Team Research Division, GhostCore Systems] **Date**: [April 2025] **Submission Target**: CERT, CISA, relevant blockchain security oversight agencies

### **Executive Summary**

This document discloses a novel attack vector within blockchain infrastructure, dubbed **"Bitcoin Kidnapping"**. It leverages manipulation of **Pay-to-Witness (P2WPKH)** transaction chains, enabling false validation of Bitcoin transactions that never occurred.

By forging witness scripts and aligning them with phantom UTXO entries, attackers may simulate high-value transactions without actual coin transfer. When executed correctly, the blockchain's own consensus mechanisms validate the forged transaction, creating the illusion of a legitimate payment.

### **Threat Profile**

**Vector Name**: Bitcoin Kidnapping via Witness Forgery  
 **Type**: Transaction-level Blockchain Forgery  
 **Exploitation Class**: Phantom UTXO Injection / Witness Chain Hijacking

#### **Objectives**

* Simulate legitimate transaction receipts.
* Redirect real transactions to attacker-controlled wallets.
* Abuse consensus verification layers to bypass audit trails.

#### **Affected Systems**

* Bitcoin ATMs
* Cryptocurrency exchanges
* Cold Wallet processors with simplified verification logic
* UTXO-based privacy wallets

### **Technical Breakdown**

#### **1. Phantom UTXO Collection**

Attacker aggregates unspent dust outputs from historical transactions across the blockchain. These are not spent but referenced in future witness chains.

#### **2. Witness Chain Fabrication**

Using knowledge of base58 and Bech32 encoding, attacker constructs forged witness scripts with valid structure but referencing phantom data.

#### **3. Validator Hijacking**

If the attacker controls a sufficient number of confirming nodes or targets a low-latency exchange node, the transaction gets accepted before rollback protections trigger.

#### **4. Ghost Confirmation**

Via timing attacks or Sybil wallet flooding, the phantom transaction is made to appear confirmed and immutable, while no real BTC was transferred.

### **Ethical Use Case**

**Red Team Simulation:** This exploit is viable for testing financial systems, specifically cold storage validation processes, and smart contract logic integrity for high-value transfer scenarios.

Use case: Ethical breach simulation on a crypto ATM to evaluate risk from unverified dust UTXOs.

### **Mitigation Strategy**

* Enforce strict UTXO value thresholds to reject dust inputs.
* Implement time-based entropy checks on witness chains.
* Cross-reference input/output pairs against centralized mempool mirrors.
* Enforce stricter replay protection for SegWit inputs.

### **Contact**

**GhostCore Systems** – Red Team Division  
 **Email**: [REDACTED]  
 **Submission UUID**: [auto-generated on submission]

**Note:** All information provided is for educational and preventative security purposes. GhostCore Systems asserts no responsibility for unauthorized use of this research.

**END OF DOCUMENT**