

# Security Vulnerability Report

## **Title: Exposure of Sensitive Information to Unauthorized Actors**

### **Overview**

A vulnerability was discovered in the `api.gatehub.net` endpoint that results in the exposure of sensitive transaction data without requiring authentication. This issue may allow unauthorized actors to access payment details, including addresses, values, and transaction hashes, potentially violating privacy and data protection standards.

### **Type of Vulnerability**


CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

This occurs when sensitive data is accessible by users who are not authorized to view it.

### **Affected Endpoints**

The following endpoints are publicly accessible and return detailed transaction data:

- `https://api.gatehub.net/rippledata/v2/payments/BTC+rchGBxcD1A1C2tdxF6papQYZ8kjRKMYcL?limit=1000&start=2019-06-09T19%3A36%3A00.000Z`
- `https://api.gatehub.net/rippledata/v2/payments/DSH+rcXY84C4g14iFp6taFXjjQGVeHqSCh9RX?limit=1000&start=2020-04-16T08:45:00.000Z`
- `https://api.gatehub.net/rippledata/v2/payments/ETC+rDAN8tzydyNfnNf2bfUQY6iR96UbpvNsze?limit=1000&start=2020-04-16T08:45:00.000Z`
- `https://api.gatehub.net/rippledata/v2/payments/ETH+rcA8X3TVMST1n3CJeAdGk1RdRCHii7N2h?limit=1000&start=2020-04-16T08:45:00.000Z`

 Many more similar endpoints are affected across different tokens and wallet addresses.

### **Security Impact**

The exposed information could be:

Used for blockchain intelligence, wallet tracking, and deanonymization.

Leveraged in phishing attacks or targeted social engineering.

A potential violation of data protection regulations (e.g., GDPR), depending on jurisdiction.

### **Suggested Remediation**

- Implement authentication and authorization checks for sensitive endpoints.
- Provide anonymized or aggregated data to the public where full access is not necessary.
- Add rate limiting and monitoring to detect unusual access patterns.

#### Disclosure Status

Responsible disclosure followed.