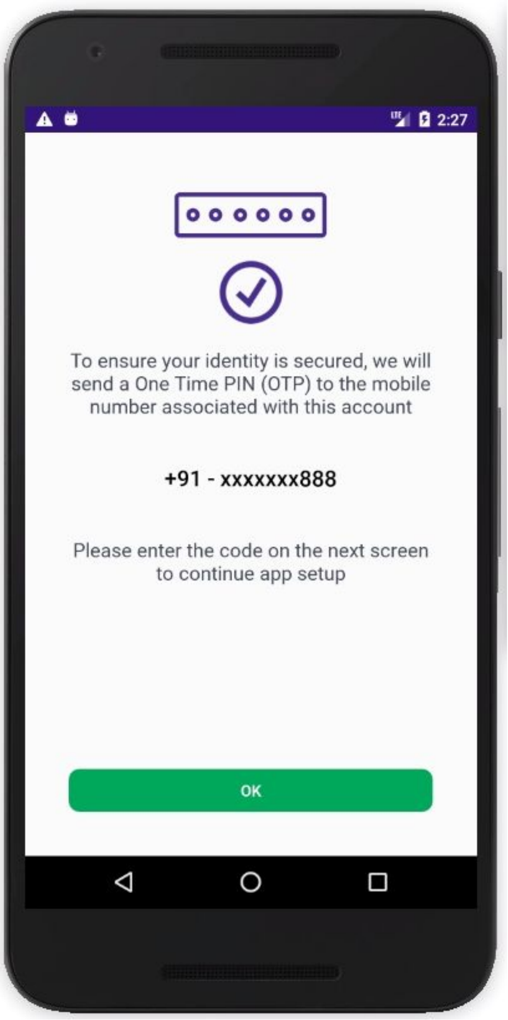
Everus.org 1.0.9 Second Factor Redirection

Vulnerability: Everus.org 1.0.9 Second Factor Redirection
Author: Muhammad Shahbaz
LinkedIn: https://www.linkedin.com/in/mr-muhammad-shahbaz/

Everus.org user phone number redirection vulnerability through SMS One-Time-Password (OTP) verification request.



To ensure your identity is secured, we will send a One Time PIN (OTP) to the mobile number associated with this account

+91 - xxxxxxx888

Please enter the code on the next screen to continue app setup

Attack Pattern:

Client can send a random phone number during the second factor flow and the server will send the OTP to that number of the requested user_id:

```
POST https://everus.org/api/mobileVerifyToSendSMS HTTP/1.1
{
   "app_name": "EVERUS",
   "mobile_no": "+XX-XXXXXXXXXX",
   "mobile_status": "0",
   "user_id": "XXXXXX"
}

Response: HTTP/1.1 200 OK
{
   "status": "Success",
   "twofacode": “”
}
```

Vulnerability Parameters:

“user_id” and “mobile_no”, by sending any existing user_id with a random phone number while requesting SMS OTP, the random phone number will receive the SMS OTP.

Vulnerability Type:

Design flaw

Vulnerability Details:

The Everus.org Android application version 1.0.9 has a fundamental design flaw where the client can send a random phone number during the second factor flow and the server will send the SMS OTP to that number.

This occurs when user requests the two factor SMS OTP from mobile app, mobile phone with user id is also being transferred from the client side of the APP and on the server side without any further authentication or verification it sends SMS OTP to that phone number of the given user id.

This is not very common vulnerability and its successful exploitation can bypass any user’s SMS second factor authentication to login.

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

Impact:

Depending on the account, an attacker can bypass any user’s second factor SMS OTP authentication to login.

Actions to Take:

SMS OTP verification on mobile apps need to be redesign with fetching mobile phone number from server side than on client side and adding preventive measures.

Vulnerability was reported to the company on Nov 15, 2018.