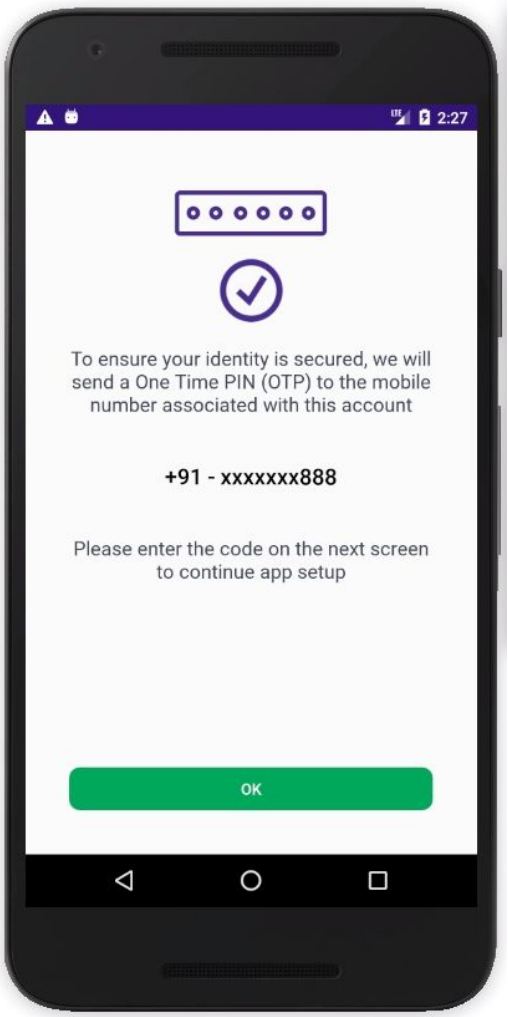
Everus.org SMS OTP Vulnerability

Vulnerability: Everus.org SMS OTP Vulnerability
Author: Muhammad Shahbaz
LinkedIn: https://www.linkedin.com/in/mr-muhammad-shahbaz/

Everus.org SMS One-Time-Password (OTP) Vulnerability in Android App.



Attack Pattern:

Capturing the request using man-in-the-middle proxy:

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": 496XXX
}
```


Vulnerability:

“twofacode” SMS OTP returned in response and compared on client side.

Vulnerability Type:

Design flaw

Vulnerability Details:

{PROBLEM} identified with SMS OTP authentication scheme in mobile app, which occurs when user requests the two factor SMS OTP from mobile app and SMS two factor one time password is also being transferred to client side of the APP. SMS OTP can be bypassed by simply capturing the response of the SMS OTP request.

This is not very common vulnerability and its successful exploitation can bypass SMS Two factor authentication.

Even though I believe this is intended feature of the mobile app which can be 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 password and other authentication protection, an attacker can easily bypass SMS two factor authentication to gain access of an account on a successful attack.
Other vulnerabilities to be considered

POSSIBLE ATTACKS	COST
SPAMMING	Price
DOS (Denial of Service)	Disruption in service and Blockage of SMS account

Actions to Take:

Two factor authentication with SMS OTP on mobile apps need to be redesign with authentication on server side than on client side and adding preventive measures.

Vulnerability was reported to the company on October 19, 2018.