CVE-2020-27414 Mahavitaran Android Application: Insecure Communication of Sensitive Data

1 Comment Uncategorized tp9222@gmail.com August 22, 2021

Vulnerable Software: Maharashtra State Electricity Board Android Application

Vulnerability: Insecure Communication of sensitive data

Affected Version: 7.50 and prior

Patched: Yes

Vendor Homepage: https://www.mahadiscom.in/en/home/

App store link: https://play.google.com/store/apps/details?id=com.msedcl.app&hl=en_IN&gl=US

CVE: CVE-2020-27414

CVE Author: Tejas Nitin Pingulkar

Exploit Available: POC Available

About Affected Software

The Official App for Consumer by Mahavitaran (M.S.E.D.C.L.). Mahavitaran Consumer App enables consumers to avail Mahavitaran services at his/her fingertips. The app is simple and easy to use. It provides transparency in delivering services to consumers.

►Features :

*View and Pay bill
*Register and Track complaints
*View Bill and Payment history
*Manage Multiple Electricity Connections
*Contact 24 x7 MSEDCL Call Center
*Apply for New Connection
* Know the status of New Connection Application and Pay Estimate Charges
*Submit Meter Reading to avoid average billing
*Provide Feedback about Mahavitaran Services
*Update Contact Details (Mobile Number & E-mail ID) of consumer
*Find MSEDCL offices and collection centers near you
*Estimate your monthly electricity consumption and bill amount
*Get Information about the Feeder from where the power supply is provided to your connection
*Apply for the change of name
*Submit an application for addition/reduction in load

Exploit

Use any proxy software such as burp
login via app

Recent Posts

Protected: Smart Office Suite- Unauthenticated Data Ex

CVE-2021-41716 Mahavitaran Android Application: Account take over via OTP Fixation

CVE-2020-27413 Mahavitaran Android Application: Clear-text password storage

CVE-2020-27416 Mahavitaran Android Application: Account take over via OTP bypass

CVE-2020-35398: UTI Mutual fund Android Application- Username Enumeration

Archives

December 2022

December 2021

September 2021

August 2021

December 2020

July 2020

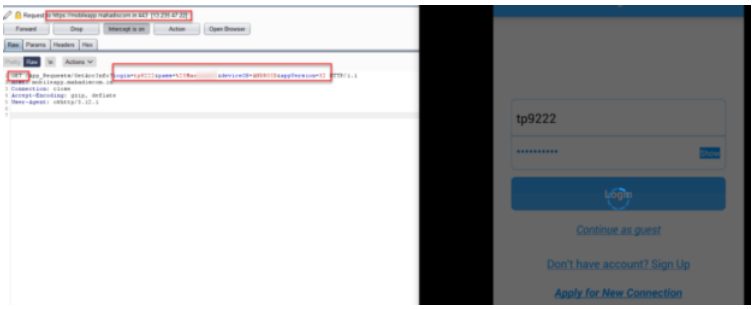
June 2020

April 2020

Gallery


intercept traffic

Observe that app sends username password as url parameter



‹ CVE-2020-13474: NCH Express Accounts- Privilege Escalation

CVE-2020-35398: UTI Mutual fund Android Application- Username Enumeration ›

One thought on “CVE-2020-27414 Mahavitaran Android Application: Insecure Communication of Sensitive Data”

Pingback: Vulnerability Summary for the Week of November 29, 2021 – Totally Secure

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment *

Name *

Email *

Website

Save my name, email, and website in this browser for the next time I comment.

Post Comment

tp9222@gmail.com +91 8149756079