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

No Comments Uncategorized tp9222@gmail.com September 23, 2021

Vulnerable Software: UTI Mutual fund Android Application

Vulnerability: Username Enumeration

Affected Version: 5.4.28

Patch: Not Released (03-December-2021)

Vendor Homepage: https://utimf.com/

CVE: CVE-2020-11561

CVE Author: Tejas Nitin Pingulkar

Exploit Available: POC available

About Affected Software

Investing in Mutual Funds is now easy with the UTI MF (UTI Mutual Funds) App. It gives you a hassle-free experience to invest in any mutual fund scheme of your choice from anywhere, anytime with just a few clicks. The paperless transactions allow new investors to start a SIP or invest a lumpsum with ease.

Exploit

Input an incorrect username (one that don't exist), the application will respond with an error message "we are unable to recognize the use user id entered" were as if the valid username is entered and invalid password is provided application responds with "the password entered is incorrect" which assist attacker to enumerate valid usernames

Proof Of Concept

First screenshot shows that user exist

Second screenshot shows that user does not exist

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

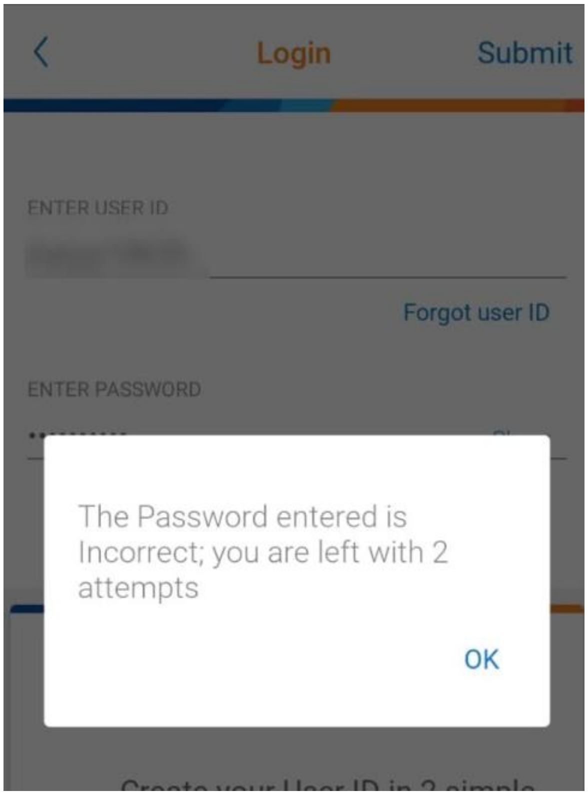
December 2020

July 2020

June 2020

April 2020

Gallery



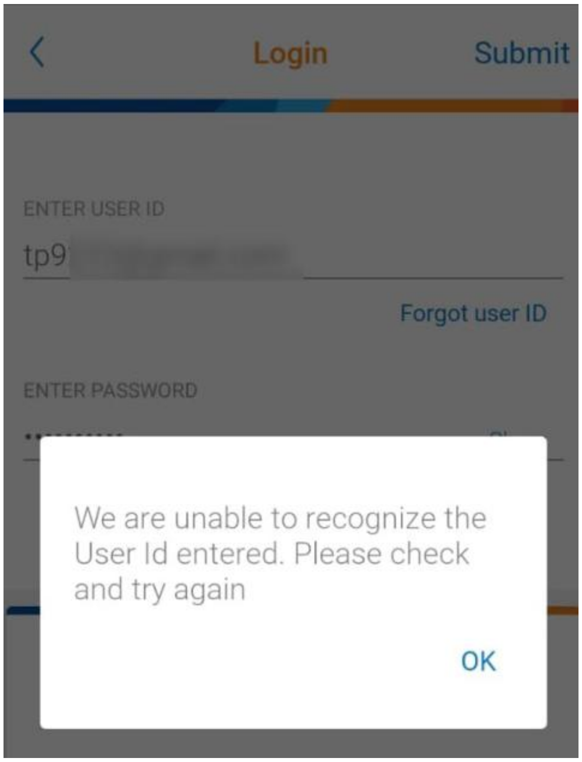
ENTER USER ID

[redacted]

ENTER PASSWORD

••••••••••

The Password entered is Incorrect; you are left with 2 attempts



ENTER USER ID

tp9[redacted]

ENTER PASSWORD

••••••••••

We are unable to recognize the User Id entered. Please check and try again

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

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

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