|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | **Account Takeover through OTP Bypass** | **Risk Rating**: High |
| **Description** | It is observed that while testing the application, mobile number field in forgot password web page is not being validated at the server side properly. | |
| **Affected Path(s)** | http://www.bima.ap.gov.in/login.aspx | |
| **Impact** | An Adversary can change the password of the user account without the knowledge of the victim and gain unauthorised access to the user account. | |
| **Evidence/Proof of Concept**  Step 1: Access the URL and navigate to Forgot Password page as shown below:  Annotation 2019-08-05 154604.png  Step 2: now enter the username an click on change password then it will ask to send otp or not then click on yes and capture request as shown in below image:  #3 Capture2.JPG  Step 3: now in captured change the original phone number to attacker phone number as shown below:  #4 Burp.JPG  Step 4:Now the OTP will be sent to attacker phone number will lead to change the password of user as shown in below image.  #4 Capture3.JPG  Step 5:Now the attacker can be able to login to user account as show in below image  #5 After login.JPG | | |
| **Recommendation** | 1. It is recommended to implement proper validation at the server side. | |
| **Management Comments** |  | |