



## ANDROID STATIC ANALYSIS REPORT

No icon



com.o-ph.prod.ct152.rejoyn\_app\_asset\_pack\_2801.apk

File Name: com.o-ph.prod.ct152.rejoyn\_app\_asset\_pack\_2801.apk

Package Name: com.o-ph.prod.ct152.rejoyn






Scan Date: Sept. 1, 2025, 6:42 a.m.

App Security Score: **85/100 (LOW RISK)**

Grade:



## FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
0	1	0	1	1

## FILE INFORMATION

**File Name:** com.opf.prod.ct152.rejoyn\_app\_asset\_pack\_2801.apk

**Size:** 196.4MB

**MD5:** a027c30009493a3152de248910d2332e

**SHA1:** 2854b3b938f40ba9b22dd5d38416ef3eee5e9272

**SHA256:** 644d0a9619f49afea4b148cad44c72ded2a989139bcddef02314c78f358b04b3

## APP INFORMATION

**App Name:**

**Package Name:** com.opf.prod.ct152.rejoyn

**Main Activity:**

**Target SDK:**

**Min SDK:**

**Max SDK:**

**Android Version Name:**

**Android Version Code:** 2801

## APP COMPONENTS

**Activities:** 0

Services: 0  
Receivers: 0  
Providers: 0  
Exported Activities: 0  
Exported Services: 0  
Exported Receivers: 0  
Exported Providers: 0

## CERTIFICATE INFORMATION

Binary is signed  
v1 signature: True  
v2 signature: True  
v3 signature: True  
v4 signature: False  
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android  
Signature Algorithm: rsassa\_pkcs1v15  
Valid From: 2024-07-08 20:45:59+00:00  
Valid To: 2054-07-08 20:45:59+00:00  
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android  
Serial Number: 0x75b1dced379dbd08da5c4f150a0c8214458471b6  
Hash Algorithm: sha256  
md5: 70ad4a6ea846a570e58b391829e7a500  
sha1: f0457087ea3144fe19800d4fd6ed61263a4036ca  
sha256: 3db9c91da9bbaa0c3799229e2b10ba9828dda176864671f2366692cdcd523cb0  
sha512: 1dca74de8e03d1f212e420d1ad9b6e27c858a9f99e2c916c7b4826012590237b75e6052a09d96dde4d74680f5ab9880aa647dd2290ee8dd3b92aa93007246bf6  
PublicKey Algorithm: rsa  
Bit Size: 4096  
Fingerprint: 95bb312cbe478cbafc1c4736fd7a7731123609d57dd6dcca3e3f21ef593868d3  
Found 1 unique certificates

## APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
------------	--------	------	-------------

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.

## NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION
----	-------	----------	-------------

## CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 0 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate

## MANIFEST ANALYSIS

HIGH: 0 | WARNING: 1 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	Application Data can be Backed up [android:allowBackup] flag is missing.	warning	The flag [android:allowBackup] should be set to false. By default it is set to true and allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.

## </> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
----	-------	----------	-----------	-------

## 📄 NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
----	------------	-------------	---------	-------------

## 🔴🔴🔴 ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	3/25	android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_PHONE_STATE, android.permission.READ_EXTERNAL_STORAGE
Other Common Permissions	0/44	

### Malware Permissions:

Top permissions that are widely abused by known malware.

Other Common Permissions:  
Permissions that are commonly abused by known malware.

## ▶ PLAYSTORE INFORMATION

**Title:** Rejoyn™

**Score:** 3.8444445 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** [com.oph.prod.ct152.rejoyn](https://play.google.com/store/apps/details?id=com.oph.prod.ct152.rejoyn)

**Developer Details:** Otsuka Precision Health, Inc., Otsuka+Precision+Health,+Inc., None, <https://www.rejoyn.com>, [Connect@otsuka-oph.com](mailto:Connect@otsuka-oph.com),

**Release Date:** Jul 25, 2024 **Privacy Policy:** [Privacy link](#)

**Description:**

Meet Rejoyn™, the first and only add-on prescription app for the treatment of major depressive disorder symptoms, also known as depression. Rejoyn is authorized by the FDA for adults age 22+ who want to add to their antidepressant medication. Over the course of 6 weeks, Rejoyn delivers proven brain-training exercises and short skills-based therapy lessons. Unlike wellness apps, Rejoyn was studied in a phase 3 clinical trial and is classified as a medical device. Rejoyn requires a prescription from a healthcare provider. The brain-training exercises in Rejoyn were developed and studied by a team of psychologists, psychiatrists, and neuroscientists. In a clinical trial, adding Rejoyn to antidepressant medication reduced depression symptoms with zero side effects related to Rejoyn. The exercises and lessons in Rejoyn tap into the brain's natural ability to change, known as neuroplasticity. You can think of it like physical therapy, but for your brain. Using Rejoyn for less than 2 hours per week for 6 weeks is designed to change how the brain works, which can improve depression symptoms. Rejoyn core functionality also includes reminders to help keep you on schedule. For example, if your treatment session is interrupted, you will be prompted to return to complete your exercise within 15 minutes so that you don't lose your progress. Interested in trying Rejoyn? Rejoyn must be prescribed by a healthcare provider. Talk to your provider about Rejoyn or learn how you can consult with a provider online at [www.rejoyn.com](https://www.rejoyn.com). Already have a prescription? Download the app to get started. Once Rejoyn is downloaded, the app will guide you through setting up your account. For more information, visit [www.rejoyn.com](https://www.rejoyn.com). See Patient Instructions for Use at <https://www.rejoyn.com/Patient-Instructions-for-Use.pdf>. INDICATION: Rejoyn is a prescription digital therapeutic for the treatment of Major Depressive Disorder (MDD) symptoms as an adjunct to clinician-managed outpatient care for adult patients with MDD age 22 years and older who are on antidepressant medication. It is intended to reduce MDD symptoms. SAFETY INFORMATION: Rejoyn is not intended to be used as a standalone treatment. Rejoyn does not replace your current medication, including medication for treatment of MDD. You should continue your current treatment as directed by your healthcare provider. Rejoyn cannot send alerts or warnings to your healthcare provider. If you feel that your depression symptoms are worsening or if you have feelings or thoughts of harming yourself or others, please contact your healthcare provider, dial 911, or go to the nearest emergency room immediately. To review the developer's Privacy Policy, visit <http://www.rejoyn.com/app-privacy-policy.html>. © 2024 Otsuka Precision Health, Inc. All rights reserved. September 2024 20US24EBC0073

## ☰ SCAN LOGS

Timestamp	Event	Error
2025-09-01 06:42:28	Generating Hashes	OK

2025-09-01 06:42:29	Extracting APK	OK
2025-09-01 06:42:29	Unzipping	OK
2025-09-01 06:42:29	Parsing APK with androguard	OK
2025-09-01 06:42:29	Extracting APK features using aapt/aapt2	OK
2025-09-01 06:42:29	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 06:42:31	Parsing AndroidManifest.xml	OK
2025-09-01 06:42:31	Extracting Manifest Data	OK
2025-09-01 06:42:31	Manifest Analysis Started	OK
2025-09-01 06:42:31	Performing Static Analysis on: com.opf.prod.ct152.rejoyn	OK
2025-09-01 06:42:32	Fetching Details from Play Store: com.opf.prod.ct152.rejoyn	OK
2025-09-01 06:42:33	Checking for Malware Permissions	OK
2025-09-01 06:42:33	Fetching icon path	OK



2025-09-01 06:42:33	Library Binary Analysis Started	OK
2025-09-01 06:42:33	Reading Code Signing Certificate	OK
2025-09-01 06:42:35	Running APKiD 2.1.5	OK
2025-09-01 06:42:41	Detecting Trackers	OK
2025-09-01 06:42:42	Decompiling APK to Java with JADX	OK
2025-09-01 06:42:43	Decompiling with JADX failed, attempting on all DEX files	OK
2025-09-01 06:42:43	Converting DEX to Smali	OK
2025-09-01 06:42:43	Code Analysis Started on - java_source	OK
2025-09-01 06:42:43	Android SBOM Analysis Completed	OK
2025-09-01 06:42:43	Android SAST Completed	OK
2025-09-01 06:42:43	Android API Analysis Started	OK
2025-09-01 06:42:44	Android API Analysis Completed	OK

2025-09-01 06:42:44	Android Permission Mapping Started	OK
2025-09-01 06:42:45	Android Permission Mapping Completed	OK
2025-09-01 06:42:45	Android Behaviour Analysis Started	OK
2025-09-01 06:42:45	Android Behaviour Analysis Completed	OK
2025-09-01 06:42:45	Extracting Emails and URLs from Source Code	OK
2025-09-01 06:42:45	Email and URL Extraction Completed	OK
2025-09-01 06:42:45	Extracting String data from Code	OK
2025-09-01 06:42:45	Extracting String values and entropies from Code	OK
2025-09-01 06:42:45	Performing Malware check on extracted domains	OK
2025-09-01 06:42:45	Saving to Database	OK

---

### Report Generated by - MobSF v4.4.0

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.