MOBSF

ANDROID STATIC ANALYSIS REPORT

STIM onTrack (3.1.0)

File Name:	com.orthofix.stimontrack_292.apk
Package Name:	com.orthofix.stimontrack
Scan Date:	Sept. 1, 2025, 6:47 a.m.
App Security Score:	45/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	2/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	11	2	0	1

FILE INFORMATION

File Name: com.orthofix.stimontrack_292.apk
Size: 11.46MB
MD5: 1094f490e73d663a3e9ab6d89fa43660
SHA1: 4d3d989635cb199016e4e5b4dda1096b1d58db79
SHA256: 10319ccb3a37a980e41ea9e211976b67aaeb604df9ad59f0894d0fc7449e9b11

APP INFORMATION

App Name: STIM onTrack
Package Name: com.orthofix.stimontrack
Main Activity: com.orthofix.stimontrack.SplashActivity
Target SDK: 33
Min SDK: 26
Max SDK:
Android Version Name: 3.1.0

Android Version Code: 292

APP COMPONENTS

Activities: 21
Services: 8
Receivers: 5
Providers: 4
Exported Activities: 0
Exported Services: 0
Exported Receivers: 1
Exported Providers: 1

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=TX, L=Lewisville, O=Orthofix, CN=Orthofix Inc
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2017-05-08 20:32:43+00:00
Valid To: 2042-05-02 20:32:43+00:00
Issuer: C=US, ST=TX, L=Lewisville, O=Orthofix, CN=Orthofix Inc
Serial Number: 0x5dbfc94
Hash Algorithm: sha256
md5: a317cbf3783c134b79516842ffe100be
sha1: 3d4135f669fba49d16b0803ad4cd364fe6620a13
sha256: 1c32c6c8214f09e36ee4cfb340d143388a12b8d1bb4f5f95c6f64c0dfdb91770
sha512: 5b4c739934963f339cb47a25a82cbf755db6f79ae4bc5e78335e31e5eabd1e00cc6e733d03c7fe61d1823b63750f7647b3520610c9b67162fefe1fe13157ade3
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: b993990def946bcedf2d28494bd61ba237356415beaddaf850ac8701eeacc97f
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.BLUETOOTH_SCAN	dangerous	required for discovering and pairing Bluetooth devices.	Required to be able to discover and pair nearby Bluetooth devices.
android.permission.BLUETOOTH_CONNECT	dangerous	necessary for connecting to paired Bluetooth devices.	Required to be able to connect to paired Bluetooth devices.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.CALL_PHONE	dangerous	directly call phone numbers	Allows the application to call phone numbers without your intervention. Malicious applications may cause unexpected calls on your phone bill. Note that this does not allow the application to call emergency numbers.
android.permission.WRITE_CALENDAR	dangerous	add or modify calendar events and send emails to guests	Allows an application to add or change the events on your calendar, which may send emails to guests. Malicious applications can use this to erase or modify your calendar events or to send emails to guests.
android.permission.READ_CALENDAR	dangerous	read calendar events	Allows an application to read all of the calendar events stored on your phone. Malicious applications can use this to send your calendar events to other people.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.orthofix.stimontrack.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check Build.MANUFACTURER check Build.DEVICE check Build.TAGS check FINDINGS: Compiler — DETAILS: r8

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Anti-VM Code</td><td>Build.MODEL check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
possible VM check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

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: 1 | WARNING: 3 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 8.0, minSdk=26]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
3	Content Provider (com.orthofix.stimontrack.utility.TestProvider) is not Protected. [android:exported=true]	warning	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
4	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

CODE ANALYSIS

HIGH: 0 | WARNING: 5 | INFO: 1 | SECURE: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bumptech/glide/Glide.java com/bumptech/glide/disklrucache/DiskLruCache.java com/bumptech/glide/gifdecoder/GifHeaderParser.java com/bumptech/glide/gifdecoder/StandardGifDecoder.java com/bumptech/glide/load/data/AssetPathFetcher.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/bumptech/glide/load/data/LocalUriFetcher.java com/bumptech/glide/load/data/mediastore/ThumbFetcher.java com/bumptech/glide/load/data/mediastore/ThumbnailStreamOpener.java com/bumptech/glide/load/engine/DecodeJob.java com/bumptech/glide/load/engine/DecodePath.java com/bumptech/glide/load/engine/Engine.java com/bumptech/glide/load/engine/GlideException.java com/bumptech/glide/load/engine/SourceGenerator.java com/bumptech/glide/load/engine/bitmap_recycle/LruArrayPool.java com/bumptech/glide/load/engine/bitmap_recycle/LruBitmapPool.java com/bumptech/glide/load/engine/cache/DiskLruCacheWrapper.java com/bumptech/glide/load/engine/cache/MemorySizeCalculator.java com/bumptech/glide/load/engine/executor/GlideExecutor.java com/bumptech/glide/load/engine/executor/Runt

NO	ISSUE	SEVERITY	STANDARDS	FILES
				imeCompat.java com/bumptech/glide/load/engine/prefill/BitmapPreFillRunner.java com/bumptech/glide/load/model/ByteBufferEncoder.java com/bumptech/glide/load/model/ByteBufferFileLoader.java com/bumptech/glide/load/model/FileLoader.java com/bumptech/glide/load/model/ResourceLoader.java com/bumptech/glide/load/model/StreamEncoder.java com/bumptech/glide/load/resource/ImageDecoderResourceDecoder.java com/bumptech/glide/load/resource/bitmap/BitmapEncoder.java com/bumptech/glide/load/resource/bitmap/BitmapImageDecoderResourceDecoder.java com/bumptech/glide/load/resource/bitmap/DefaultImageHeaderParser.java com/bumptech/glide/load/resource/bitmap/Downsampler.java com/bumptech/glide/load/resource/bitmap/DrawableToBitmapConverter.java com/bumptech/glide/load/resource/bitmap/HardwareConfigState.java com/bumptech/glide/load/resource/bitmap/TransformationUtils.java com/bumptech/glide/load/resource/bitmap/VideoDecoder.java com/bumptech/glide/load/resource/gif/ByteBufferGifDecoder.java com/bumptech/glide/load/resource/gif/GifDrawableEncoder.java com/bumptech/glide/load/resource/gif/StreamGifDecoder.java com/bumptech/glide/manager/DefaultConnectivityMonitor.java com/bumptech/glide/manager/DefaultConnectiv

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	ityMonitorFactory.java com/bumptech/glide/manager/RequestManagerFragment.java com/bumptech/glide/manager/RequestManagerRetriever.java com/bumptech/glide/manager/RequestTracker.java com/bumptech/glide/manager/SupportRequestManagerFragment.java com/bumptech/glide/module/ManifestParser.java com/bumptech/glide/request/SingleRequest.java com/bumptech/glide/request/target/CustomViewTarget.java com/bumptech/glide/request/target/ViewTarget.java com/bumptech/glide/signature/ApplicationVersionSignature.java com/bumptech/glide/util/ContentLengthInputStream.java com/bumptech/glide/util/pool/FactoryPools.java com/github/barteksc/pdfviewer/PDFView.java com/github/mikephil/charting/charts/BarChart.java com/github/mikephil/charting/charts/BarLineChartBase.java com/github/mikephil/charting/charts/Chart.java com/github/mikephil/charting/charts/CombinedChart.java com/github/mikephil/charting/charts/HorizontalBarChart.java com/github/mikephil/charting/charts/PieRadarChartBase.java com/github/mikephil/charting/components/AxisBase.java com/github/mikephil/charting/data/ChartData.java com/github/mikephil/charting/data/CombinedData.java com/github/mikephil/charting/data/LineDataSet.

NO	ISSUE	SEVERITY	STANDARDS	FILES
				java com/github/mikephil/charting/data/PieEntry.java com/github/mikephil/charting/listener/BarLineChartTouchListener.java com/github/mikephil/charting/renderer/ScatterChartRenderer.java com/github/mikephil/charting/utils/FileUtils.java com/github/mikephil/charting/utils/Utils.java com/orm/SchemaGenerator.java com/orm/SugarDb.java com/orm/SugarRecord.java com/orm/SugarTransactionHelper.java com/orm/util/ManifestHelper.java com/orm/util/ReflectionUtil.java com/orm/util/SugarCursorFactory.java com/orthofix/stimontrack/BaseActivity.java com/orthofix/stimontrack/BasePresenter.java com/orthofix/stimontrack/flows/main/CareReportWebActivity.java com/orthofix/stimontrack/flows/main/HeartRatesChartActivity.java com/orthofix/stimontrack/flows/main/ResourcesWebActivity.java com/orthofix/stimontrack/flows/main/fragments/CalendarFragment.java com/orthofix/stimontrack/flows/main/fragments/ChartsContainerFragment.java com/orthofix/stimontrack/flows/main/fragments/TreatmentFragment.java com/orthofix/stimontrack/flows/main/fragments/charts/ChartsPageTwoFragment.java com/orthofix/stimontrack/flows/main/fragments/charts/chartFragments/HeartRatesChartFragment.java com/orthofix/stimontrack/flows/main/fragments/charts/chartFragments/PainChartFragment.java com/orthofix/stimontrack/flows/main/fragments/charts/chartFragments/StepsChartFragment.java com/orthofix/stimontrack/flows/main/fragments

NO	ISSUE	SEVERITY	STANDARDS	FILES
				/charts/chartFragments/TreatmentHistoryChartFragment.java com/orthofix/stimontrack/flows/main/fragments/healthapis/LoginFibitActivity.java com/orthofix/stimontrack/flows/main/fragments/healthapis/LoginGarminActivity.java com/orthofix/stimontrack/flows/main/fragments/treatment/VASQuestionnaireFragment.java com/orthofix/stimontrack/flows/main/fragments/treatment/healthapis/LoginFibitActivity.java com/orthofix/stimontrack/flows/main/fragments/treatment/healthapis/LoginGarminActivity.java com/orthofix/stimontrack/flows/main/healthtracker/HealthTrackerActivity.java com/orthofix/stimontrack/flows/pairdevice/PairDeviceActivity.java com/orthofix/stimontrack/flows/pairdevice/PairDevicePresenter.java com/orthofix/stimontrack/flows/settings/SettingsActivity.java com/orthofix/stimontrack/flows/settings/SettingsPresenter.java com/orthofix/stimontrack/models/DeviceInfo.java com/orthofix/stimontrack/utility/AlarmReceiver.java com/orthofix/stimontrack/utility/BleService.java com/orthofix/stimontrack/utility/BluetoothStatusReceiver.java com/orthofix/stimontrack/utility/OrthofixNotificationMessagingService.java com/orthofix/stimontrack/utility/SystemManager.java com/orthofix/stimontrack/utility/UploadDataToServer.java com/pierfrancescosoffritti/androidyoutubeplayer/player/a.java com/pierfrancescosoffritti/androidyoutubeplayer/ui/menu/defaultMenu/DefaultYouTubePlayerMenu.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/bumptech/glide/load/Option.java com/bumptech/glide/load/engine/DataCacheKey.java com/bumptech/glide/load/engine/EngineResource.java com/bumptech/glide/load/engine/ResourceCacheKey.java com/bumptech/glide/manager/RequestManagerRetriever.java com/orthofix/stimontrack/flows/main/fragments/healthapis/LoginFibitActivity.java com/orthofix/stimontrack/flows/main/fragments/healthapis/LoginGarminActivity.java com/orthofix/stimontrack/flows/main/fragments/treatment/healthapis/LoginFibitActivity.java com/orthofix/stimontrack/flows/main/fragments/treatment/healthapis/LoginGarminActivity.java com/orthofix/stimontrack/utility/SystemManager.java com/orthofix/stimontrack/utility/UploadDataToServer.java
3	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	com/orthofix/stimontrack/flows/main/fragments/healthapis/LoginFibitActivity.java com/orthofix/stimontrack/flows/main/fragments/healthapis/LoginGarminActivity.java com/orthofix/stimontrack/flows/main/fragments/treatment/healthapis/LoginFibitActivity.java com/orthofix/stimontrack/flows/main/fragments/treatment/healthapis/LoginGarminActivity.java com/pierfrancescosoffritti/androidyoutubeplayer/player/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/orthofix/stimontrack/flows/main/fragments/healthapis/LoginGarminActivity.java com/orthofix/stimontrack/flows/main/fragments/treatment/healthapis/LoginGarminActivity.java
5	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/orm/SchemaGenerator.java com/orm/SugarRecord.java
6	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/github/mikephil/charting/charts/Chart.java com/github/mikephil/charting/utils/FileUtils.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00091	Retrieve data from broadcast	collection	com/orthofix/stimontrack/flows/main/healthtracker/HealthTrackerActivity.java
00022	Open a file from given absolute path of the file	file	com/github/mikephil/charting/charts/Chart.java com/orm/util/MultiDexHelper.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/orthofix/stimontrack/BasePresenter.java com/orthofix/stimontrack/flows/main/CareReportWebActivity.java com/orthofix/stimontrack/flows/main/fragments/HelpFragment.java com/orthofix/stimontrack/utility/SystemManager.java com/pierfrancescosoffritti/androidyoutubeplayer/ui/DefaultPlayerUIController.java
00112	Get the date of the calendar event	collection calendar	com/orm/util/ReflectionUtil.java com/orthofix/stimontrack/utility/BleService.java com/orthofix/stimontrack/utility/SystemManager.java
00089	Connect to a URL and receive input stream from the server	command network	com/bumptech/glide/load/data/HttpUrlFetcher.java com/orthofix/stimontrack/flows/main/CareReportWebActivity.java
00030	Connect to the remote server through the given URL	network	com/bumptech/glide/load/data/HttpUrlFetcher.java com/orthofix/stimontrack/flows/main/CareReportWebActivity.java
00109	Connect to a URL and get the response code	network command	com/bumptech/glide/load/data/HttpUrlFetcher.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/bumptech/glide/load/data/mediastore/ThumbFetcher.java
00147	Get the time of current location	collection location	com/orthofix/stimontrack/utility/SystemManager.java

RULE ID	BEHAVIOUR	LABEL	FILES
00104	Check if the given path is directory	file	com/orthofix/stimontrack/utility/SystemManager.java
00036	Get resource file from res/raw directory	reflection	com/orthofix/stimontrack/utility/SystemManager.java
00096	Connect to a URL and set request method	command network	com/orthofix/stimontrack/flows/main/CareReportWebActivity.java
00072	Write HTTP input stream into a file	command network file	com/orthofix/stimontrack/flows/main/CareReportWebActivity.java
00094	Connect to a URL and read data from it	command network	com/orthofix/stimontrack/flows/main/CareReportWebActivity.java
00108	Read the input stream from given URL	network command	com/orthofix/stimontrack/flows/main/CareReportWebActivity.java
00013	Read file and put it into a stream	file	com/bumptech/glide/disklrucache/DiskLruCache.java com/bumptech/glide/load/ImageHeaderParserUtils.java com/bumptech/glide/load/model/FileLoader.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://android-stimontrack-71af5.firebaseio.com

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/343444788625/namespaces/firebase:fetch?key=AIzaSyCbde7_AASe2EjYCF5ID7BCLhNJka9DRvY is enabled. Ensure that the configurations are not sensitive. This is indicated by the response: {'entries': {'AccelStim_Videos': '"7fGYOMinAdo,Fc98ld7UfnQ,JNhMGN5MT5E"', 'Accel_Videos': '696565852?h=6b636101eb,1109474348,1109474718', 'Android_Minimum_Version_Supported': '101', 'AppRating_NoOfTimes_Decline': '2', 'AppRating_TreatmentDays_Condition': '5', 'AppRating_WaitTime_ConditionInMin': '1', 'CareReport_Disclaimer': 'I understand that I may download my personal health information for my own personal use, or to share with my health care provider. Orthofix is not responsible for any subsequent unauthorized use or disclosure of my personal health information once I have directed it to be shared with a third party. Orthofix will only share my personal information with my explicit authorization, except as otherwise specified in the Notice of Privacy Practices.', 'CareReport_Disclaimer_Accept_Button': 'I Understand', 'CareReport_Disclaimer_Deny_Button': 'Cancel', 'CareReport_disclaimer_Title': 'Caution', 'CervicalStim_Videos': '"pL79licnQmA,QUScqo3lCLw,ZElbBCYwxRw,vZpqrj2i5D8,Fc98ld7UfnQ,JNhMGN5MT5E"', 'Cervical_Videos': '258609714,198746142,374152364,116821330,1109474348,1109474718', 'Clinical_Link_Faq': 'https://www.orthofix.com/wp-content/uploads/2020/01/Frequently_Asked_Questions_RCStim.pdf', 'Clinical_Link_Manual': 'https://www.orthofix.com/wp-content/uploads/2020/01/Subject_Manual_RCStim.pdf', 'Firmware_Version': '', 'How_Pemf_Works': '"lkcf3EzKbaA"', 'LEFI_Instructions': 'Although you may consider two of the statements in any one section relate to you, please mark the box that closely describes your present–day / current situation.', 'LEFI_Introduction': 'The Lower Extremity Functional Scale (LEFS) Questionnaire is designed to help your physician better understand whether you are having any difficulty with the activities listed due to your lower limb condition for which you are currently seeking attention. Mark in each section the one box that applies to you. ', 'LEFI_SectionHeader': 'Today, do you or would you have any difficulty at all with:', 'Legend_Interpretation_NDI_ODI': 'Please answer every section. Choose only one answer in each section that most closely describes you today.', 'Legend_Interpretation_UEFI_LEFS': 'Please answer every section. Choose only one answer in each section that most closely describes you today.', 'Link_AndroidHelp_Calendar': 'https://bonegrowththerapy.com/stim-ontrack-troubleshooting', 'Link_AndroidHelp_Charts': 'https://ontrackproduction.orthofix.com:8090', 'Link_AndroidHelp_PairScreen': 'https://bonegrowththerapy.com/resources/manuals-downloads', 'Link_AndroidHelp_Resources': 'https://bonegrowththerapy.com/stim-ontrack-troubleshooting', 'Link_AndroidHelp_TrackerConnect': 'https://docs.google.com/gview?embedded=true&url=https://bonegrowththerapy.com/wp-content/uploads/2025/03/FAQ_ActivityTracker_FNL.pdf', 'Link_AndroidHelp_TrackerData': 'https://ontrackproduction.orthofix.com:8091', 'Link_AndroidHelp_Treatment': 'https://bonegrowththerapy.com/stim-ontrack-troubleshooting', 'Link_BoneGrowthTherapy': 'https://bonegrowththerapy.com', 'Link_Email': 'https://rndproduction.orthofix.com/sotmessaging', 'Link_Email_dev': 'https://ontrackdev.orthofix.com/SOTMessaging', 'Link_Faq': 'https://bonegrowththerapy.com/resources/faqs', 'Link_Fitbit': 'https://store.google.com/category/watches_trackers?hl=en-US', 'Link_Garmin': 'https://connect.garmin.com', 'Link_PatientGuide': 'https://bonegrowththerapy.com/wp-content/uploads/2023/10/BS-2415-STIM-onTrack-3.2-onTrack-Instructional-Guide-Update-v28-CLEAN.pdf', 'Lipus_Video': '745081672?h=74de9f82cf', 'Models_Hide_PROM_2_1': '"5404"', 'Models_Hide_PROM_Tab': '"5404,5303,5313,5314,5315,5302,5212,5505"', 'NDI_Instructions': 'ALTHOUGH YOU MAY CONSIDER THAT TWO OF THE STATEMENTS IN ANY ONE SECTION RELATE TO YOU, PLEASE CHOOSE THE STATEMENT THAT <STRONG>MOST CLOSELY</STRONG> DESCRIBES YOUR PRESENT-DAY SITUATION.', 'NDI_Introduction': 'THIS QUESTIONNAIRE IS DESIGNED TO HELP US BETTER UNDERSTAND HOW YOUR NECK PAIN AFFECTS YOUR ABILITY TO MANAGE EVERYDAY-LIFE ACTIVITIES. PLEASE SELECT IN EACH SECTION THE ONE STATEMENT THAT APPLIES TO YOU.', 'NDI_SectionHeader': 'Please select in the section the one box that applies to you. Although you may consider that two of the statements relate to you, please select the statement that most closely describes your present-day situation.', 'NDI_survey_internet_link': "Internet: https://eprovide.mapi-trust.org", 'ODI_Instructions': 'Please answer every section. Choose only one answer in each section that most closely describes you today.', 'ODI_Introduction': 'This questionnaire is designed to give us information as to how your back (or leg) trouble affects your ability to

TITLE	SEVERITY	DESCRIPTION
		'ODI_Introduction': 'This questionnaire is designed to give us information as to how your back (or leg) trouble affects your ability to manage in everyday life.', 'ODI_SectionHeader': 'Select the answer that most closely describes you today.', 'ODI_survey_internet_link': 'Internet: https://eprovide.mapi-trust.org', 'Pemf_Video': '258125681', 'PhysioStim_Videos': '"pL79licnQmA,IJSQpj09QfE,iv8ClrC1fL4,N4eyvABfzF0,Fc98ld7UfnQ,JNhMGN5MT5E"', 'Physio_Videos': '258609714,258141537,16926873?h=d858d9c568,116821329,1109474348,1109474718', 'Show_Tracker_Tab': 'true', 'Source_LEFI': '© 1996, J. Binkley, reprinted with permission.', 'Source_NDI': 'NDI © Dr. Howard Vernon, 1991. All Rights Reserved. ', 'Source_ODI': 'ODI © Jeremy Fairbank, 1980. All Rights Reserved. ', 'Source_UEFI': '© 2001, P. Stratford, reprinted with permission.', 'SpinalStim_Videos': '"pL79licnQmA,dMPAgR_G4eo,zTl_PG4e6n8,VfOdKDk-0FQ,Fc98ld7UfnQ,JNhMGN5MT5E"', 'Spinal_Videos': '258609714,198747036,116821328,392749943,1109474348,1109474718', 'UEFI_Instructions': 'Although you may consider two of the statements in any one section related to you, please mark the box that closely describes your present–day / current situation.', 'UEFI_Introduction': 'The Upper Extremity Functional Index (UEFI) Questionnaire is designed to help your physician better understand whether you are having any difficulty with the activities listed below due to your upper limb condition for which you are currently seeking attention. Mark in each section the one box that applies to you. ', 'UEFI_SectionHeader': 'Today, do you or would you have any difficulty at all with:', 'UEFI_survey_internet_link': '', 'Update_Encryption_Pair_Popup': 'Please pair with your STIM device by scanning the bar code or entering the serial number manually.', 'days_HR_diaplay': '7', 'days_Steps_display': '7', 'help_header_image_label': 'How it Works', 'help_header_image_link': 'https://ontrackProduction.orthofix.com/Android_images/how-it-works.png', 'help_header_image_lipus_video_link': '"rFhmd8QGNsc"', 'help_header_image_video_link': '"Ikcf3EzKbaA"', 'privacy_url': 'https://ontrackverification.orthofix.com/OTC/', 'privacy_url_dev': 'https://ontrackverification.orthofix.com/OTC/', 'survey_contact_LEFI': 'Source: Binkley JM, Stratford PW, Lott SA, Riddle DL. The Lower Extremity Functional Scale (LEFS): scale development, measurement properties, and clinical application. North American Orthopaedic Rehabilitation Research Network. Phys Ther. 1999 Apr;79(4):371-83.', 'survey_contact_NDI': 'For any information on the use of the NDI, please contact Mapi Research Trust, Lyon, France.', 'survey_contact_ODI': 'For any information on the use of the ODI, please contact Mapi Research Trust, Lyon, France.', 'survey_contact_UEFI': 'Source: Stratford PW, Binkley, JM, Stratford DM (2001): Development and initial validation of the upper extremity functional index. Physiotherapy Canada.'}, 'state': 'UPDATE', 'templateVersion': '80'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	8/25	android.permission.CAMERA, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION, android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE, android.permission.WAKE_LOCK
Other Common Permissions	6/44	android.permission.BLUETOOTH, android.permission.BLUETOOTH_ADMIN, android.permission.CALL_PHONE, android.permission.READ_CALENDAR, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

TYPE	MATCHES	PERMISSIONS

Malware Permissions:
Top permissions that are widely abused by known malware.
Other Common Permissions:
Permissions that are commonly abused by known malware.

! OFAC SANCTIONED COUNTRIES

This app may communicate with the following OFAC sanctioned list of countries.

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
www.nairday.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
play.google.com	ok	**IP:** 142.250.74.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
facebook.com	ok	**IP:** 31.13.70.36 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
linkedin.com	ok	**IP:** 150.171.22.12 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
twitter.com	ok	**IP:** 172.66.0.227 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
web.orthofix.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.google.com	ok	**IP:** 142.250.74.68 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
api.fitbit.com	ok	**IP:** 216.58.207.202 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
docs.google.com	ok	**IP:** 216.58.214.78 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.bonestimulation.com	ok	**IP:** 15.197.225.128 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.youtube.com	ok	**IP:** 216.58.213.78 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
connectapi.garmin.com	ok	**IP:** 104.17.152.222 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
ontrackproduction.orthofix.com	ok	**IP:** 199.47.90.33 **Country:** United States of America **Region:** Texas **City:** Irving **Latitude:** 32.889099 **Longitude:** -96.942802 **View:** Google Map
connect.garmin.com	ok	**IP:** 104.17.167.14 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
direct.orthofix.com	ok	**IP:** 104.18.11.170 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
android-stimontrack-71af5.firebaseio.com	ok	**IP:** 34.120.206.254 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
bonegrowththerapy.com	ok	**IP:** 34.148.232.130 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map
instagram.com	ok	**IP:** 31.13.70.174 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.bonegrowththerapy.com	ok	**IP:** 34.148.232.130 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map
www.fitbit.com	ok	**IP:** 35.244.211.136 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

TRACKERS

TRACKER	CATEGORIES	URL
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

HARDCODED SECRETS

POSSIBLE SECRETS
"firebase_database_url" : "https://android-stimontrack-71af5.firebaseio.com"
"google_api_key" : "AIzaSyCbde7_AASe2EjYCF5lD7BCLhNJka9DRvY"
"google_crash_reporting_api_key" : "AIzaSyCbde7_AASe2EjYCF5lD7BCLhNJka9DRvY"
"precribed_time_key" : "KEY_PRESCRIBED_TIME"
uywFHQIUTVQYfmxNjcl5x4Ry8Gihzl3Y7jf
6a878ea484d346d1ee45f5c16ddaa3b6
05028d14-3c71-4138-9151-555de1f530ed
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
470fa2b4ae81cd56ecbcda9735803434cec591fa

PLAYSTORE INFORMATION

Title: STIM onTrack ™ App

Score: 4.537671 **Installs:** 50,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.orthofix.stimontrack

Developer Details: Orthofix BioStim, Orthofix+BioStim, None, http://BoneGrowthTherapy.com, STIMonTrackSupport@Orthofix.com,

Release Date: Mar 30, 2018 **Privacy Policy:** Privacy link

Description:

Orthofix Bone Growth Stimulation Therapy devices are prescribed by physicians to improve fracture healing and spinal fusion success rates. The STIM onTrack™ mobile app provides tools and information for patients to help them use their bone growth therapy device daily as prescribed by their physician. STIM onTrack app features for

patients: • Create a daily treatment reminder • View a duplicate display of their device • Daily treatment calendar • Integration with activity trackers to read and display Steps and Resting Heart Rate averages. • Connect with an Orthofix Sales Rep or Patient Services with one-touch calling • Send message to Patient Care • Link to read answers to commonly asked questions • Learn how Orthofix Bone Growth Stimulation Therapy devices help improve fracture healing and spinal fusion success rates • Access to standardized Patient Reported Outcomes Measure (PROM) questionnaires For more information, visit BoneGrowthTherapy.com STIM onTrack mobile app is intended for U.S. Residents only.

SCAN LOGS

Timestamp	Event	Error
2025-09-01 06:47:28	Generating Hashes	OK
2025-09-01 06:47:28	Extracting APK	OK
2025-09-01 06:47:28	Unzipping	OK
2025-09-01 06:47:28	Parsing APK with androguard	OK
2025-09-01 06:47:28	Extracting APK features using aapt/aapt2	OK
2025-09-01 06:47:29	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 06:47:30	Parsing AndroidManifest.xml	OK

2025-09-01 06:47:30	Extracting Manifest Data	OK
2025-09-01 06:47:30	Manifest Analysis Started	OK
2025-09-01 06:47:30	Performing Static Analysis on: STIM onTrack (com.orthofix.stimontrack)	OK
2025-09-01 06:47:32	Fetching Details from Play Store: com.orthofix.stimontrack	OK
2025-09-01 06:47:33	Checking for Malware Permissions	OK
2025-09-01 06:47:33	Fetching icon path	OK
2025-09-01 06:47:33	Library Binary Analysis Started	OK
2025-09-01 06:47:33	Reading Code Signing Certificate	OK
2025-09-01 06:47:34	Running APKiD 2.1.5	OK
2025-09-01 06:47:37	Detecting Trackers	OK
2025-09-01 06:47:39	Decompiling APK to Java with JADX	OK

2025-09-01 06:47:53	Converting DEX to Smali	OK
2025-09-01 06:47:53	Code Analysis Started on - java_source	OK
2025-09-01 06:47:54	Android SBOM Analysis Completed	OK
2025-09-01 06:47:59	Android SAST Completed	OK
2025-09-01 06:47:59	Android API Analysis Started	OK
2025-09-01 06:48:02	Android API Analysis Completed	OK
2025-09-01 06:48:02	Android Permission Mapping Started	OK
2025-09-01 06:48:06	Android Permission Mapping Completed	OK
2025-09-01 06:48:06	Android Behaviour Analysis Started	OK
2025-09-01 06:48:10	Android Behaviour Analysis Completed	OK
2025-09-01 06:48:10	Extracting Emails and URLs from Source Code	OK

2025-09-01 06:48:10	Email and URL Extraction Completed	OK
2025-09-01 06:48:10	Extracting String data from APK	OK
2025-09-01 06:48:10	Extracting String data from Code	OK
2025-09-01 06:48:10	Extracting String values and entropies from Code	OK
2025-09-01 06:48:13	Performing Malware check on extracted domains	OK
2025-09-01 06:48:18	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.