



ANDROID STATIC ANALYSIS REPORT



 UpToDate (3.70.4)

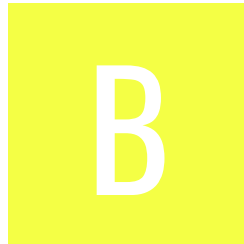
File Name: com.uptodate.android_167.apk

Package Name: com.uptodate.android

Scan Date: Sept. 1, 2025, 11:04 a.m.






App Security Score: 43/100 (MEDIUM RISK)

Grade:



Trackers Detection: 5/432

FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
7	22	2	2	2

FILE INFORMATION

File Name: com.uptodate.android_167.apk

Size: 37.49MB

MD5: 488a78554a9c17cdc41b9e938e5c8c57

SHA1: ae76f391ceab8ac80d48e3965cd1030373b7cf50

SHA256: af235e14e9c3a3c29e4ebab2ddb0e2ecffb6fe586ca28fd583b1819b69d20459

APP INFORMATION

App Name: UpToDate

Package Name: com.uptodate.android

Main Activity: com.uptodate.android.PermissionAcceptanceActivity

Target SDK: 34

Min SDK: 28

Max SDK:

Android Version Name: 3.70.4

Android Version Code: 167

APP COMPONENTS

Activities: 56

Services: 7

Receivers: 7

Providers: 3

Exported Activities: 5

Exported Services: 0

Exported Receivers: 4

Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed

v1 signature: False

v2 signature: True

v3 signature: False

v4 signature: False

X.509 Subject: C=US, ST=MA, L=Waltham, O=UpToDate, OU=UpToDate, CN=Jim Ronan

Signature Algorithm: rsassa_pkcs1v15

Valid From: 2012-05-04 17:32:45+00:00

Valid To: 2039-09-20 17:32:45+00:00

Issuer: C=US, ST=MA, L=Waltham, O=UpToDate, OU=UpToDate, CN=Jim Ronan

Serial Number: 0x4fa412bd

Hash Algorithm: sha1

md5: 5fc02ac68ea53d32a481f242f46ee98f

sha1: dc9d63793b0598b8b2b49bab34830af9d5a196d3

sha256: 21d3a5feb68ce06171eeae569f4f5e59d9b29cbbe809dff77c8ad7b7d0c884bc

sha512: ba1b4f7bceae54b69e5ed5c6b9ecc42ce66dd5c3d318c24145a4fe298246fd45fc5ba60ec411704a42e9765e83afead7149326b53ed30658404c66e8686296c3

PublicKey Algorithm: rsa

Bit Size: 2048

Fingerprint: 5f45a1e79b005f8df3fa5b1aae11122028bf0c918fa5924bb6a0245f1e99c373

Found 1 unique certificates

≡ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
com.android.launcher.permission.INSTALL_SHORTCUT	unknown	Unknown permission	Unknown permission from android reference
com.android.launcher.permission.UNINSTALL_SHORTCUT	unknown	Unknown permission	Unknown permission from android reference
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.uptodate.android.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

FILE	DETAILS	
488a78554a9c17cdc41b9e938e5c8c57.apk	FINDINGS	DETAILS
	Anti-VM Code	possible VM check
classes.dex	FINDINGS	DETAILS
	yara_issue	yara issue - dex file recognized by apkid but not yara module
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.TAGS check
	Compiler	unknown (please file detection issue!)

FILE	DETAILS	
classes2.dex		
	FINDINGS	DETAILS
	yara_issue	yara issue - dex file recognized by apkid but not yara module
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.BRAND check Build.DEVICE check Build.PRODUCT check Build.HARDWARE check Build.BOARD check Build.TAGS check network operator name check possible VM check
	Anti Debug Code	Debug.isDebuggerConnected() check
	Compiler	unknown (please file detection issue!)

FILE	DETAILS	
classes3.dex	FINDINGS	DETAILS
	yara_issue	yara issue - dex file recognized by apkid but not yara module
	Compiler	unknown (please file detection issue!)
classes4.dex	FINDINGS	DETAILS
	yara_issue	yara issue - dex file recognized by apkid but not yara module
	Anti-VM Code	Build.MANUFACTURER check Build.BOARD check SIM operator check
	Compiler	unknown (please file detection issue!)

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.uptodate.android.LaunchActivity	Schemes: uptodate://,
sdk.pendo.io.activities.PendoGateActivity	Schemes: pendo-13ce367c://,

NETWORK SECURITY

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

CERTIFICATE ANALYSIS

HIGH: 1 | WARNING: 0 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Certificate algorithm vulnerable to hash collision	high	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues.

MANIFEST ANALYSIS

HIGH: 1 | WARNING: 11 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 9, minSdk=28]	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.

NO	ISSUE	SEVERITY	DESCRIPTION
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	Application Data can be Backed up [android:allowBackup=true]	warning	This flag 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.
4	Broadcast Receiver (com.appsflyer.MultipleInstallBroadcastReceiver) is not Protected. [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.
5	Broadcast Receiver (com.uptodate.android.NetworkStateReceiver) is not Protected. [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.
6	Broadcast Receiver (com.uptodate.android.SearchWidgetProvider) is not Protected. [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.
7	Activity (com.uptodate.android.LaunchActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
8	Activity (com.uptodate.android.SearchShortcutActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
9	Activity (com.uptodate.android.CalculatorShortcutActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
10	Activity (sdk.pendo.io.activities.PendoGateActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
11	Activity (androidx.compose.ui.tooling.PreviewActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
12	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [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: 4 | WARNING: 9 | INFO: 1 | SECURE: 2 | SUPPRESSED: 0

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

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/sun/jna/Native.java net/bytebuddy/dynamic/DynamicType.java org/glassfish/jersey/message/internal/FileProvider.java org/glassfish/jersey/message/internal/Utils.java org/h2/engine/Database.java org/h2/engine/SessionRemote.java org/h2/engine/UndoLog.java org/h2/mvstore/db/MVTempResult.java org/h2/result/RowList.java org/h2/store/fs/FilePathRec.java org/h2/store/fs/FilePathWrapper.java org/h2/store/fs/FilePathZip.java org/h2/store/fs/FileUtils.java org/h2/upgrade/DbUpgrade.java org/h2/value/ValueLobDb.java org/junit/rules/TemporaryFolder.java org/springframework/cglib/transform/AbstractTransformTask.java org/springframework/http/codec/multipart/PartGenerator.java
				butterknife/ButterKnife.java com/appsflyer/AppsFlyerLib.java com/appsflyer/MultipleInstallBroadcastReceiver.java com/appsflyer/TestReceiver.java com/appsflyer/cache/a.java com/appsflyer/f.java com/bumptech/glide/b.java com/bumptech/glide/diskruncache/a.java com/bumptech/glide/gifdecoder/d.java com/bumptech/glide/gifdecoder/e.java com/bumptech/glide/load/data/b.java com/bumptech/glide/load/data/j.java com/bumptech/glide/load/data/l.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bumptech/glide/load/data/mediastore/c.java com/bumptech/glide/load/data/mediastore/e.java com/bumptech/glide/load/engine/bitmap_recycle/i.java com/bumptech/glide/load/engine/bitmap_recycle/j.java com/bumptech/glide/load/engine/cache/e.java com/bumptech/glide/load/engine/cache/i.java com/bumptech/glide/load/engine/executor/a.java com/bumptech/glide/load/engine/h.java com/bumptech/glide/load/engine/i.java com/bumptech/glide/load/engine/k.java com/bumptech/glide/load/engine/q.java com/bumptech/glide/load/engine/z.java com/bumptech/glide/load/model/c.java com/bumptech/glide/load/model/d.java com/bumptech/glide/load/model/f.java com/bumptech/glide/load/model/r.java com/bumptech/glide/load/model/s.java com/bumptech/glide/load/resource/a.java com/bumptech/glide/load/resource/bitmap/b0.java com/bumptech/glide/load/resource/bitmap/c.java com/bumptech/glide/load/resource/bitmap/d.java com/bumptech/glide/load/resource/bitmap/k.java com/bumptech/glide/load/resource/bitmap/m.java com/bumptech/glide/load/resource/bitmap/n.java com/bumptech/glide/load/resource/bitmap/r.java com/bumptech/glide/load/resource/bitmap/z.java com/bumptech/glide/load/resource/gif/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bumptech/glide/load/resource/gif/d.java com/bumptech/glide/load/resource/gif/j.java com/bumptech/glide/manager/RequestManagerFragment.java com/bumptech/glide/manager/SupportRequestManagerFragment.java com/bumptech/glide/manager/f.java com/bumptech/glide/manager/o.java com/bumptech/glide/manager/q.java com/bumptech/glide/manager/r.java com/bumptech/glide/module/d.java com/bumptech/glide/request/h.java com/bumptech/glide/request/target/i.java com/bumptech/glide/util/pool/a.java com/caverock/androidsvg/SVGImageView.java com/caverock/androidsvg/b.java com/caverock/androidsvg/i.java com/caverock/androidsvg/l.java com/qualtrics/digital/ActionSet.java com/qualtrics/digital/DateExpression.java com/qualtrics/digital/DayExpression.java com/qualtrics/digital/DurationExpression.java com/qualtrics/digital/InterceptDefinition.java com/qualtrics/digital/Properties.java com/qualtrics/digital/Qualtrics.java com/qualtrics/digital/QualtricsLog.java com/qualtrics/digital/QualtricsPopOverFragment.java com/qualtrics/digital/QualtricsSurveyActivity.java com/qualtrics/digital/QualtricsSurveyExpression.java com/qualtrics/digital/ServiceInterceptor.java com/qualtrics/digital/TimeExpression.java com/qualtrics/digital/VariableExpression.java com/qualtrics/digital/ViewCountExpression.java com/qualtrics/digital/WebViewInterface.java com/qualtrics/digital/resolvers/CustomPropertyResolver.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/qualtrics/digital/resolvers/DateTimeTypeR esolvers.java com/qualtrics/digital/resolvers/QualtricsSurve yResolver.java com/qualtrics/digital/resolvers/SamplingResol ver.java com/qualtrics/digital/resolvers/TimeSpentInAp pResolver.java com/qualtrics/digital/resolvers/ViewCountReso lver.java com/sun/jna/platform/win32/COM/tlb/TlbImp. java com/sun/jna/platform/win32/COM/tlb/imp/Tlb Base.java com/sun/jna/platform/win32/COM/tlb/imp/Tlb CmdlineArgs.java com/uptodate/android/CalculatorShortcutActiv ity.java com/uptodate/android/DBHelperBase.java com/uptodate/android/LaunchActivity.java com/uptodate/android/NetworkStateReceiver.j ava com/uptodate/android/SearchShortcutActivity.j ava com/uptodate/android/SearchWidgetProvider.j ava com/uptodate/android/UtdApplication.java com/uptodate/android/async/AsyncMessagePr ocessor2.java com/uptodate/android/async/AsyncMessageTa sk2.java com/uptodate/android/calculators/Calculators ListActivity.java com/uptodate/android/client/AndroidProgress Listener.java com/uptodate/android/client/BookmarkAndHi storyEventProcessingJob.java com/uptodate/android/client/ExternalFileMana ger.java com/uptodate/android/client/StorageServiceAn

NO	ISSUE	SEVERITY	STANDARDS	FILES
				droid.java com/uptodate/android/client/UtdClientAndroid com/uptodate/android/cme/CMEBaseActivity.j ava com/uptodate/android/content/AppActionInter face.java com/uptodate/android/content/AsyncTopicBu ndleAssetTask.java com/uptodate/android/content/DisclosuresList Activity.java com/uptodate/android/content/DrugContribut orDisclosureActivity.java com/uptodate/android/content/DrugInteractio nViewActivity.java com/uptodate/android/content/EmailActivity.ja va com/uptodate/android/content/ExternalURLW ebViewActivity.java com/uptodate/android/content/FormularyActi vity.java com/uptodate/android/content/FragmentTable OfContents.java com/uptodate/android/content/InternalLinkAct ivity.java com/uptodate/android/content/PeerReviewers ListActivity.java com/uptodate/android/content/TopicContribut orsActivity.java com/uptodate/android/content/UtdWebView.j ava com/uptodate/android/content/ViewCitationAc tivity.java com/uptodate/android/content/ViewGraphicAc tivity.java com/uptodate/android/content/ViewHtmlAsset Activity.java com/uptodate/android/content/ViewTopicActiv ity\$client\$1.java com/uptodate/android/content/ViewTopicActiv

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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	ity\$loadTopicTaskCallBack\$1.java com/uptodate/android/content/ViewTopicActivity.java com/uptodate/android/home/HomeWithMenuActivity.java com/uptodate/android/html/a.java com/uptodate/android/login/LoginActivity.java com/uptodate/android/login/NewLoginActivity.java com/uptodate/android/provider/ScrollPositionProvider.java com/uptodate/android/provider/TopicStack.java com/uptodate/android/provider/UtClientAndroidProvider.java com/uptodate/android/search/AsyncTaskAutoCompleteSuggestion.java com/uptodate/android/search/AsyncTaskSearchResults.java com/uptodate/android/search/AsyncTaskSynonym.java com/uptodate/android/search/FragmentFrequentlyUsedList.java com/uptodate/android/search/SearchHandler.java com/uptodate/android/search/SpeechHandlerDialog.java com/uptodate/android/search/UtSearchManager.java com/uptodate/android/settings/DevelopersActivity.java com/uptodate/android/settings/FragmentManagerPreferences.java com/uptodate/android/settings/ManageMyDevicesActivity.java com/uptodate/android/settings/SelectLanguageActivity.java com/uptodate/android/sync/DownloadOptionsActivity.java com/uptodate/android/sync/SyncIntentService.

NO	ISSUE	SEVERITY	STANDARDS	<div>java</div> <div>FILES</div> <div>com/uptodate/android/tools/AppOsStaleCheck er.java</div>
				<div>com/uptodate/android/tools/DialogFactory.jav a</div> <div>com/uptodate/android/tools/FrequentlyUsedT racker.java</div> <div>com/uptodate/android/tools/ThroughputCheck er.java</div> <div>com/uptodate/android/tools/ToastUtility.java</div> <div>com/uptodate/android/ui/DrugInteractionsUtil. java</div> <div>com/uptodate/android/ui/PathwaysInteraction sUtil.java</div> <div>com/uptodate/android/ui/floatingsearchview/ util/Util.java</div> <div>com/uptodate/android/useractivity/AsyncHisto ryEventsRequest.java</div> <div>com/uptodate/android/useractivity/FragmentH istory.java</div> <div>com/uptodate/android/useractivity/UserBook marksAndHistoryActivity.java</div> <div>com/uptodate/app/client/UtdClient.java</div> <div>com/uptodate/app/client/services/EventServic e.java</div> <div>com/uptodate/app/client/tools/SystemOutPro gressListener.java</div> <div>com/uptodate/tools/Md5Tool.java</div> <div>com/uptodate/tools/PatternTool.java</div> <div>com/uptodate/vo/XmlElement.java</div> <div>com/uptodate/vo/event/Event.java</div> <div>com/uptodate/vo/logging/EventType.java</div> <div>external/sdk/pendo/io/com/appmattus/certific atetransparency/internal/loglist/model/v2/Log \$\$serializer.java</div> <div>external/sdk/pendo/io/glide/a.java</div> <div>external/sdk/pendo/io/glide/gifdecoder/Standa rdGifDecoder.java</div> <div>external/sdk/pendo/io/glide/gifdecoder/d.java</div> <div>external/sdk/pendo/io/glide/load/data/AssetPa</div>

NO	ISSUE	SEVERITY	STANDARDS	FILES
				<div>thFetcher.java</div> <div>external/sdk/pendo/io/glide/load/data/HttpUr iFetcher.java</div> <div>external/sdk/pendo/io/glide/load/data/LocalUr iFetcher.java</div> <div>external/sdk/pendo/io/glide/load/data/medias tore/ThumbFetcher.java</div> <div>external/sdk/pendo/io/glide/load/data/medias tore/c.java</div> <div>external/sdk/pendo/io/glide/load/engine/Engin e.java</div> <div>external/sdk/pendo/io/glide/load/engine/bitm ap_recycle/LruArrayPool.java</div> <div>external/sdk/pendo/io/glide/load/engine/bitm ap_recycle/LruBitmapPool.java</div> <div>external/sdk/pendo/io/glide/load/engine/cach e/DiskLruCacheWrapper.java</div> <div>external/sdk/pendo/io/glide/load/engine/g.jav a</div> <div>external/sdk/pendo/io/glide/load/engine/h.jav a</div> <div>external/sdk/pendo/io/glide/load/engine/n.jav a</div> <div>external/sdk/pendo/io/glide/load/engine/u.jav a</div> <div>external/sdk/pendo/io/glide/load/model/Byte BufferEncoder.java</div> <div>external/sdk/pendo/io/glide/load/model/Byte BufferFileLoader.java</div> <div>external/sdk/pendo/io/glide/load/model/FileL oader.java</div> <div>external/sdk/pendo/io/glide/load/model/Reso urceLoader.java</div> <div>external/sdk/pendo/io/glide/load/model/Strea mEncoder.java</div> <div>external/sdk/pendo/io/glide/load/resource/Im ageDecoderResourceDecoder.java</div> <div>external/sdk/pendo/io/glide/load/resource/bit map/BitmapEncoder.java</div> <div>external/sdk/pendo/io/glide/load/resource/bit</div>

NO	ISSUE	SEVERITY	STANDARDS	map/BitmapImageDecoderResourceDecoder.java FILES external/sdk/pendo/io/glide/load/resource/bit
				map/DefaultImageHeaderParser.java external/sdk/pendo/io/glide/load/resource/bit map/VideoDecoder.java external/sdk/pendo/io/glide/load/resource/bit map/b.java external/sdk/pendo/io/glide/load/resource/bit map/c.java external/sdk/pendo/io/glide/load/resource/bit map/d.java external/sdk/pendo/io/glide/load/resource/gif/ ByteBufferGifDecoder.java external/sdk/pendo/io/glide/load/resource/gif/ GifDrawableEncoder.java external/sdk/pendo/io/glide/load/resource/gif/ StreamGifDecoder.java external/sdk/pendo/io/glide/manager/DefaultC onnectivityMonitorFactory.java external/sdk/pendo/io/glide/manager/b.java external/sdk/pendo/io/glide/request/SingleReq uest.java external/sdk/pendo/io/glide/request/target/Cu stomViewTarget.java external/sdk/pendo/io/glide/request/target/Vie wTarget.java external/sdk/pendo/io/mozilla/javascript/Scrip tRuntime.java external/sdk/pendo/io/mozilla/javascript/tools /debugger/Dim.java external/sdk/pendo/io/mozilla/javascript/tools /idswitch/Main.java external/sdk/pendo/io/mozilla/javascript/tools /jsc/Main.java jakarta/activation/h.java org/eclipse/angus/activation/LogSupport.java org/eclipse/angus/activation/nativeimage/Ang usActivationFeature.java org/glassfish/hk2/classmodel/reflect/util/Direc

NO	ISSUE	SEVERITY	STANDARDS	FILES
				toryArchive.java org/glassfish/hk2/osgiresourcelocator/ServiceLoaderImpl.java org/glassfish/hk2/utilities/reflection/Logger.java org/h2/engine/Session.java org/h2/engine/UndoLogRecord.java org/h2/mvstore/db/LobStorageMap.java org/h2/mvstore/tx/TransactionStore.java org/h2/pagestore/PageStore.java org/h2/pagestore/db/LobStorageBackend.java org/h2/server/TcpServer.java org/h2/server/pg/PgServer.java org/h2/server/web/WebServer.java org/h2/store/FileStore.java org/h2/util/AbbaLockingDetector.java org/h2/util/IOUtils.java org/h2/util/MathUtils.java org/h2/util/Profiler.java org/koin/android/logger/AndroidLogger.java org/koin/core/logger/EmptyLogger.java org/koin/core/time/MeasureKt.java org/slf4j/helpers/Util.java org/springframework/cglib/core/DebuggingClassWriter.java org/springframework/cglib/reflect/FastMethod.java org/springframework/core/SpringProperties.java org/springframework/util/SystemPropertyUtils.java org/springframework/web/util/ServletContextPropertyUtils.java org/sqlroid/Log.java org/sqlroid/SQLDroidBlob.java org/sqlroid/SQLDroidConnection.java org/sqlroid/SQLDroidDatabaseMetaData.java org/sqlroid/SQLDroidDriver.java org/sqlroid/SQLDroidPreparedStatement.java org/sqlroid/SQLDroidResultSet.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				org/sqlroid/SQLDroidResultSetMetaData.java org/sqlroid/SQLDroidStatement.java org/sqlroid/SQLiteDatabase.java
				sdk/pendo/io/PendoInternal.java sdk/pendo/io/activities/PendoGateActivity.java sdk/pendo/io/c0/j.java sdk/pendo/io/c0/k.java sdk/pendo/io/c0/m.java sdk/pendo/io/c0/n.java sdk/pendo/io/g3/c.java sdk/pendo/io/h0/a.java sdk/pendo/io/i8/e.java sdk/pendo/io/j0/a.java sdk/pendo/io/j7/g.java sdk/pendo/io/logging/PendoLogger.java
				com/bumptech/glide/load/engine/d.java com/bumptech/glide/load/engine/p.java com/bumptech/glide/load/engine/x.java com/bumptech/glide/load/h.java com/qualtrics/digital/EmbeddedFeedbackUtils.java com/qualtrics/digital/ExpressionDeserializer.java com/qualtrics/digital/QualtricsPopOverFragment.java com/qualtrics/digital/XMDUtils.java com/sun/jna/platform/unix/X11.java com/sun/jna/platform/win32/PdhUtil.java com/uptodate/android/client/UtdClientAndroid.java com/uptodate/android/content/EmailActivity.java com/uptodate/android/content/ExternalURLWebViewActivity.java com/uptodate/android/content/ViewTopicActivity.java com/uptodate/android/content/terms_of_use/TermsOfUseFragmentDialog.java com/uptodate/android/home/HomeWithMenuActivity.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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/uptodate/android/login/NewLoginActivity.java com/uptodate/android/sync/SyncIntentService.java com/uptodate/android/util/PreferencesUtil.java com/uptodate/app/client/UtdClient.java com/uptodate/app/client/services/CmeLogService.java com/uptodate/web/api/Asset.java com/uptodate/web/api/LocalAppMessage.java external/sdk/pendo/io/com/appmattus/certificate/transparency/internal/loglist/model/v2/Log.java external/sdk/pendo/io/glide/load/engine/c.java external/sdk/pendo/io/glide/load/engine/m.java external/sdk/pendo/io/glide/load/engine/s.java external/sdk/pendo/io/mozilla/javascript/ClassCache.java external/sdk/pendo/io/mozilla/javascript/NativeError.java external/sdk/pendo/io/mozilla/javascript/NativeJavaObject.java external/sdk/pendo/io/mozilla/javascript/ScriptRuntime.java external/sdk/pendo/io/mozilla/javascript/xmlimpl/XmlNode.java org/glassfish/hk2/utilities/BuilderHelper.java org/glassfish/hk2/utilities/DescriptorImpl.java org/glassfish/jersey/ExternalProperties.java org/glassfish/jersey/SslConfigurator.java org/glassfish/jersey/client/ClientProperties.java org/glassfish/jersey/client/authentication/HttpAuthenticationFeature.java org/glassfish/jersey/internal/l10n/Localizer.java org/h2/engine/Constants.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				org/h2/security/CipherFactory.java org/springframework/beans/factory/support/AutowireCandidateQualifier.java org/springframework/beans/factory/support/PropertiesBeanDefinitionReader.java org/springframework/context/support/LiveBeansView.java org/springframework/http/codec/protobuf/ProtobufCodecSupport.java org/springframework/jmx/export/naming/IdentityNamingStrategy.java org/springframework/jmx/support/JmxUtils.java org/springframework/web/util/WebUtils.java sdk/pendo/io/actions/ActivationManager.java sdk/pendo/io/actions/FloatingVisualGuide.java sdk/pendo/io/actions/ToolTipVisualGuide.java sdk/pendo/io/actions/handlers/PendoGlobalCommandHandler.java sdk/pendo/io/d1/e.java sdk/pendo/io/events/IdentificationData.java sdk/pendo/io/m/d.java sdk/pendo/io/models/GlobalEventPropertiesKt.java sdk/pendo/io/models/StepModel.java sdk/pendo/io/n/b.java sdk/pendo/io/q/g.java sdk/pendo/io/views/custom/videoplayer/PendoYouTubePlayer.java org/glassfish/jersey/ssl/Configurator.java org/glassfish/jersey/client/internal/HttpURLConnection.java sdk/pendo/io/f3/c.java sdk/pendo/io/f3/d.java sdk/pendo/io/f3/g.java sdk/pendo/io/f3/h.java sdk/pendo/io/k/d.java sdk/pendo/io/t4/c.java sdk/pendo/io/t4/p0.java
4	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	

NO	ISSUE	SEVERITY	STANDARDS	FILES
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/uptodate/android/DBHelperBase.java com/uptodate/android/client/StorageServiceAndroid.java org/sqlroid/SQLiteDatabase.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/uptodate/android/client/ExternalFileManager.java com/uptodate/android/client/GuidManager.java com/uptodate/android/client/StorageServiceAndroid.java com/uptodate/android/client/UtdClientAndroid.java com/uptodate/android/util/UtdFileUtil.java sdk/pendo/io/PendoInternal.java sdk/pendo/io/r8/a.java
7	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	com/uptodate/android/util/DeviceRootCheckUtil.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
8	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/appsflyer/e.java com/github/zagum/speechrecognitionview/animations/b.java com/qualtrics/digital/SamplingUtil.java net/bytebuddy/ByteBuddy.java net/bytebuddy/agent/builder/AgentBuilder.java net/bytebuddy/dynamic/TypeResolutionStrategy.java net/bytebuddy/utility/RandomString.java org/h2/command/dml/Optimizer.java org/h2/engine/Session.java org/h2/server/web/WebApp.java org/junit/runner/manipulation/Ordering.java org/springframework/util/AlternativeJdkIdGenerator.java org/springframework/util/MimeTypeUtils.java org/springframework/util/SocketUtils.java sdk/pendo/io/j3/d.java sdk/pendo/io/j3/h.java sdk/pendo/io/j4/f.java sdk/pendo/io/v4/c.java sdk/pendo/io/v4/d.java sdk/pendo/io/w2/z.java
9	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/qualtrics/digital/QualtricsSurveyFragment.java com/uptodate/android/content/UtdWebView.java com/uptodate/android/home/HomeWithMenuActivity.java com/uptodate/android/search/KPPResultsAdapter.java sdk/pendo/io/views/custom/videoplayer/PendoYoutubePlayer.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
10	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/appsflyer/AppsFlyerLib.java com/sun/jna/platform/win32/WinCrypt.java com/uptodate/android/settings/DevelopersActivity.java external/sdk/pendo/io/mozilla/javascript/tools/debugger/Dim.java org/h2/util/NetUtils.java sdk/pendo/io/a4/b.java sdk/pendo/io/b4/b.java sdk/pendo/io/d4/b.java sdk/pendo/io/e4/d.java sdk/pendo/io/e4/f.java sdk/pendo/io/e4/k.java sdk/pendo/io/f4/h.java sdk/pendo/io/j/b.java sdk/pendo/io/jj.java sdk/pendo/io/k/i.java sdk/pendo/io/n3/b.java sdk/pendo/io/o3/a.java sdk/pendo/io/r3/a.java sdk/pendo/io/s3/a.java sdk/pendo/io/v3/b.java sdk/pendo/io/x3/a.java sdk/pendo/io/y3/a.java sdk/pendo/io/z3/a.java
11	Debug configuration enabled. Production builds must not be debuggable.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	external/sdk/pendo/io/daimajia/BuildConfig.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
12	MD5 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/appsflyer/HashUtils.java com/uptodate/app/client/tools/UserDataDecryptor.java com/uptodate/tools/Md5Tool.java external/sdk/pendo/io/mozilla/javascript/tools/shell/Main.java org/glassfish/jersey/client/authentication/DigestAuthenticator.java
13	Insecure Implementation of SSL. Trusting all the certificates or accepting self signed certificates is a critical Security Hole. This application is vulnerable to MITM attacks	high	CWE: CWE-295: Improper Certificate Validation OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	com/uptodate/app/client/UtdRestClient.java
14	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	com/uptodate/app/client/tools/Settings.java
15	Calling Cipher.getInstance("AES") will return AES ECB mode by default. ECB mode is known to be weak as it results in the same ciphertext for identical blocks of plaintext.	high	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-2	com/uptodate/app/client/tools/UserDataDecryptor.java
16	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	org/glassfish/jersey/client/authentication/DigestAuthenticator.java org/h2/util/MathUtils.java sdk/pendo/io/g9/o.java

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

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	com/bumptech/glide/disklruache/a.java com/bumptech/glide/load/f.java com/bumptech/glide/load/model/f.java com/uptodate/android/client/ExternalFileManager.java com/uptodate/android/client/UtdClientAndroid.java com/uptodate/android/settings/DevelopersActivity.java com/uptodate/app/client/services/StorageService.java com/uptodate/tools/CompressionTool.java com/uptodate/tools/FileTool.java com/uptodate/tools/Md5Tool.java com/uptodate/tools/ZipFileBuilder.java external/sdk/pendo/io/glide/load/a.java external/sdk/pendo/io/glide/load/model/FileLoader.java external/sdk/pendo/io/mozilla/javascript/tools/SourceReader.java external/sdk/pendo/io/mozilla/javascript/tools/debugger/Dim.java external/sdk/pendo/io/mozilla/javascript/tools/idswitch/Main.java external/sdk/pendo/io/mozilla/javascript/tools/shell/Global.java javax/ws/rs/client/k.java javax/ws/rs/ext/d.java net/bytebuddy/build/Plugin.java net/bytebuddy/dynamic/ClassFileLocator.java net/bytebuddy/dynamic/DynamicType.java net/bytebuddy/utility/FileSystem.java org/glassfish/hk2/classmodel/reflect/util/DirectoryArchive.java org/glassfish/jersey/SslConfigurator.java org/glassfish/jersey/message/internal/FileProvider.java org/glassfish/jersey/server/internal/scanning/FileSchemeResourceFinderFactory.java org/glassfish/jersey/server/internal/scanning/FilesScanner.java

RULE ID	BEHAVIOUR	LABEL	FILES
			org/glassfish/jersey/server/internal/scanning/JarZipSchemeResourceFinderFactory.java org/glassfish/jersey/server/wadl/internal/generators/WadlGeneratorApplicationDoc.java
			org/glassfish/jersey/server/wadl/internal/generators/WadlGeneratorGrammarsSupport.java org/glassfish/jersey/server/wadl/internal/generators/resourcedoc/WadlGeneratorResourceDocSupport.java org/h2/store/fs/FilePathDisk.java org/h2/util/Profiler.java org/h2/util/SourceCompiler.java org/junit/experimental/max/MaxHistory.java org/objectweb/asm/util/CheckClassAdapter.java org/objectweb/asm/util/Printer.java org/springframework/cglib/transform/AbstractTransformTask.java sdk/pendo/io/g9/j.java sdk/pendo/io/p/a.java sdk/pendo/io/t4/m1.java sdk/pendo/io/t4/n0.java
00091	Retrieve data from broadcast	collection	com/qualtrics/digital/QualtricsNotificationManager.java com/uptodate/android/LaunchActivity.java com/uptodate/android/content/ViewTableOfContentsActivity.java com/uptodate/android/content/ViewTopicActivity.java com/uptodate/android/home/HomeWithMenuActivity.java com/uptodate/android/search/SearchActivity.java com/uptodate/android/search/SearchResultsActivity.java com/uptodate/android/settings/menu/MenuActivity.java com/uptodate/android/sync/SyncIntentService.java

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	com/sun/jna/Native.java com/sun/jna/NativeLibrary.java com/sun/jna/platform/mac/MacFileUtils.java com/sun/jna/platform/win32/Advapi32Util.java com/sun/jna/platform/win32/W32FileMonitor.java com/sun/jna/platform/win32/W32FileUtils.java com/uptodate/android/DBHelperBase.java com/uptodate/android/client/ExternalFileManager.java com/uptodate/android/client/StorageServiceAndroid.java com/uptodate/android/client/UtdClientAndroid.java com/uptodate/android/content/ViewGraphicActivity.java com/uptodate/android/html/a.java com/uptodate/android/settings/DevelopersActivity.java com/uptodate/android/util/UtdFileUtil.java com/uptodate/app/client/SyncService.java com/uptodate/app/client/dao/UnidexDao.java com/uptodate/app/client/services/StorageServiceH2.java com/uptodate/app/client/services/StorageServiceSqlite.java com/uptodate/app/client/services/UnidexService.java com/uptodate/app/client/tools/Settings.java com/uptodate/app/client/vo/DeltaItem.java com/uptodate/tools/Md5Tool.java com/uptodate/tools/ZipFileBuilder.java external/sdk/pendo/io/mozilla/javascript/tools/jsc/Main.java org/glassfish/hk2/classmodel/reflect/util/DirectoryArchive.java org/h2/server/web/WebServer.java org/h2/store/fs/FilePathDisk.java org/h2/upgrade/DbUpgrade.java org/h2/util/SourceCompiler.java org/h2/value/ValueLob.java org/springframework/cglib/transform/AbstractProcessTask.java org/springframework/cglib/transform/AbstractTransformTask.java org/springframework/core/io/FileSystemResource.java org/springframework/core/io/support/PathMatchingResourcePatternResolver.java org/springframework/web/multipart/commons/CommonsMultipartFile.java sdk/pendo/io/g9/j.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/opsflyer/AppsFlyerLib.java com/qualtrics/digital/QualtricsNotificationManager.java com/qualtrics/digital/QualtricsPopOverActivity.java com/qualtrics/digital/QualtricsSurveyFragment.java com/uptodate/android/UtdExceptionHandler.java com/uptodate/android/content/ContentFeedbackActivity.java com/uptodate/android/content/EmailActivity.java com/uptodate/android/content/ExternalURLWebViewActivity.java com/uptodate/android/content/ViewGraphicActivity.java com/uptodate/android/content/ViewHtmlAssetActivity.java com/uptodate/android/content/terms_of_use/TermsOfUseFragmentManagerDialog.java com/uptodate/android/home/FeedbackActivity.java com/uptodate/android/home/FragmentHomeMenu.java com/uptodate/android/home/HomeWithMenuActivity.java com/uptodate/android/home/helpers/i.java com/uptodate/android/login/LoginActivity.java com/uptodate/android/login/MergeAccountNotice.java com/uptodate/android/login/NewLoginActivity.java com/uptodate/android/login/UCCLoginPolicyDialog.java com/uptodate/android/search/FragmentSearchResults.java com/uptodate/android/settings/menu/PrivacyPolicySectionsExtractor.java com/uptodate/android/tools/DialogFactory.java com/uptodate/android/tools/EmailHandler.java com/uptodate/android/tools/NewDialogFactory\$ExternalLinkDialog\$2.java com/uptodate/android/tools/NotificationUtility.java sdk/pendo/io/actions/handlers/PendoGlobalCommandHandler.java
00163	Create new Socket and connecting to it	socket	org/h2/security/CipherFactory.java org/h2/server/TcpServer.java org/h2/util/NetUtils.java sdk/pendo/io/f3/b.java sdk/pendo/io/f3/h.java sdk/pendo/io/t4/b1.java
00094	Connect to a URL and read data from it	command network	com/uptodate/android/util/PDFUtil.java external/sdk/pendo/io/mozilla/javascript/tools/shell/Global.java

RULE ID	BEHAVIOUR	LABEL	FILES
00012	Read data and put it into a buffer stream	file	org/glassfish/hk2/classmodel/reflect/util/DirectoryArchive.java org/glassfish/jersey/message/internal/FileProvider.java org/springframework/cglib/transform/AbstractTransformTask.java sdk/pendo/io/t4/m1.java sdk/pendo/io/t4/n0.java
00202	Make a phone call	control	com/uptodate/android/content/ExternalURLWebViewActivity.java com/uptodate/android/content/ViewHtmlAssetActivity.java
00203	Put a phone number into an intent	control	com/uptodate/android/content/ExternalURLWebViewActivity.java com/uptodate/android/content/ViewHtmlAssetActivity.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/qualtrics/digital/QualtricsNotificationManager.java com/uptodate/android/UtdExceptionHandler.java com/uptodate/android/content/EmailActivity.java com/uptodate/android/content/ExternalURLWebViewActivity.java com/uptodate/android/content/ViewHtmlAssetActivity.java com/uptodate/android/search/FragmentSearchResults.java com/uptodate/android/tools/EmailHandler.java com/uptodate/android/tools/NotificationUtility.java
00130	Get the current WIFI information	wifi collection	sdk/pendo/io/l8/d.java
00065	Get the country code of the SIM card provider	collection	com/uptodate/android/search/autosuggest/service/AutoSuggestService.java com/uptodate/android/util/FirebaseRemoteConfigUtil.java sdk/pendo/io/l8/e.java

RULE ID	BEHAVIOUR	LABEL	FILES
00096	Connect to a URL and set request method	command network	com/appsflyer/AppsFlyerLib.java com/uptodate/android/util/PDFUtil.java com/uptodate/app/client/UtdRestClient.java org/springframework/core/io/AbstractFileResolvingResource.java org/springframework/http/client/SimpleClientHttpRequestFactory.java org/springframework/remoting/httpinvoker/SimpleHttpInvokerRequestExecutor.java
00089	Connect to a URL and receive input stream from the server	command network	com/appsflyer/AppsFlyerLib.java com/bumptech/glide/load/data/j.java com/uptodate/android/search/autosuggest/service/AutoSuggestService.java com/uptodate/android/util/PDFUtil.java com/uptodate/app/client/UtdRestClient.java external/sdk/pendo/io/glide/load/data/HttpUrlFetcher.java external/sdk/pendo/io/mozilla/javascript/commons/module/provider/UrlModuleSourceProvider.java org/springframework/core/io/UrlResource.java org/springframework/remoting/httpinvoker/SimpleHttpInvokerRequestExecutor.java
00109	Connect to a URL and get the response code	network command	com/appsflyer/AppsFlyerLib.java com/bumptech/glide/load/data/j.java com/uptodate/app/client/UtdRestClient.java external/sdk/pendo/io/glide/load/data/HttpUrlFetcher.java external/sdk/pendo/io/mozilla/javascript/commons/module/provider/UrlModuleSourceProvider.java org/springframework/core/io/AbstractFileResolvingResource.java org/springframework/remoting/httpinvoker/SimpleHttpInvokerRequestExecutor.java
00112	Get the date of the calendar event	collection calendar	com/uptodate/app/client/UtdClient.java
00189	Get the content of a SMS message	sms	com/appsflyer/AppsFlyerLib.java
00078	Get the network operator name	collection telephony	com/appsflyer/AppsFlyerLib.java com/uptodate/android/client/UtdClientAndroid.java

RULE ID	BEHAVIOUR	LABEL	FILES
00188	Get the address of a SMS message	sms	com/appsflyer/AppsFlyerLib.java
00009	Put data in cursor to JSON object	file	com/appsflyer/AppsFlyerLib.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/appsflyer/AppsFlyerLib.java
00123	Save the response to JSON after connecting to the remote server	network command	com/appsflyer/AppsFlyerLib.java com/uptodate/android/search/autosuggest/service/AutoSuggestService.java
00158	Connect to a URL and send sensitive data got from resolver	privacy connection	com/appsflyer/AppsFlyerLib.java
00030	Connect to the remote server through the given URL	network	com/appsflyer/AppsFlyerLib.java com/bumptechnology/glide/load/data/j.java com/uptodate/android/search/autosuggest/service/AutoSuggestService.java com/uptodate/android/util/PDFUtil.java external/sdk/pendo/io/glide/load/data/HttpUrlFetcher.java external/sdk/pendo/io/mozilla/javascript/commonjs/module/provider/UrlModuleSourceProvider.java
00010	Read sensitive data(SMS, CALLLOG) and put it into JSON object	sms calllog collection	com/appsflyer/AppsFlyerLib.java
00092	Send broadcast	command	com/appsflyer/AppsFlyerLib.java
00191	Get messages in the SMS inbox	sms	com/appsflyer/AppsFlyerLib.java com/uptodate/android/content/EmailActivity.java
00200	Query data from the contact list	collection contact	com/appsflyer/AppsFlyerLib.java

RULE ID	BEHAVIOUR	LABEL	FILES
00201	Query data from the call log	collection callog	com/appsflyer/AppsFlyerLib.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms callog calendar	com/appsflyer/AppsFlyerLib.java com/bumptech/glide/load/data/mediastore/c.java external/sdk/pendo/io/glide/load/data/mediastore/ThumbFetcher.java
00036	Get resource file from res/raw directory	reflection	com/appsflyer/AppsFlyerLib.java com/uptodate/android/UtdExceptionHandler.java
00054	Install other APKs from file	reflection	com/uptodate/android/util/PDFUtil.java
00072	Write HTTP input stream into a file	command network file	com/uptodate/android/util/PDFUtil.java
00108	Read the input stream from given URL	network command	com/uptodate/android/util/PDFUtil.java org/glassfish/jersey/client/internal/URLConnectionor.java
00114	Create a secure socket connection to the proxy address	network command	sdk/pendo/io/b3/f.java
00162	Create InetAddress object and connecting to it	socket	org/h2/security/CipherFactory.java org/h2/util/NetUtils.java sdk/pendo/io/f3/b.java sdk/pendo/io/f3/h.java sdk/pendo/io/t4/b1.java
00121	Create a directory	file command	com/uptodate/android/settings/DevelopersActivity.java
00125	Check if the given file path exist	file	com/uptodate/android/settings/DevelopersActivity.java
00104	Check if the given path is directory	file	com/uptodate/android/settings/DevelopersActivity.java

RULE ID	BEHAVIOUR	LABEL	FILES
00025	Monitor the general action to be performed	reflection	com/uptodate/android/login/NewLoginActivity.java
00181	Load native libraries(.so) via System.load (60% means caught)	so	net/bytebuddy/dynamic/loading/ClassInjector.java org/h2/tools/Shell.java
00157	Instantiate new object using reflection, possibly used for dexClassLoader	reflection dexClassLoader	javassist/util/proxy/g.java
00032	Load external class	reflection	org/springframework/context/support/ContextTypeMatchClassLoader.java
00024	Write file after Base64 decoding	reflection file	com/uptodate/android/content/ViewGraphicActivity.java
00047	Query the local IP address	network collection	sdk/pendo/io/t4/e1.java
00180	Load native libraries(.so) via System.loadLibrary (60% means caught)	so	net/bytebuddy/dynamic/loading/ClassInjector.java
00023	Start another application from current application	reflection control	com/uptodate/android/tools/GenericUIMethods.java

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://uptodate-5183f.firebaseio.com
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebase-remoteconfig.firebaseio.com/v1/projects/479517410060/namespaces/firebase:fetch?key=AlzaSyC2HGA1oOlho-k9RIHlrq-bnBOL5II2Ge4 is enabled. Ensure that the configurations are not sensitive. This is indicated by the response: {'entries': {'DrugHierarchyOutlineV2': 'true', 'HOMESCREEN_2025': 'true', 'LoginRedesign': 'true', 'MissingGASearchResultNonFATALs': '{ "searchTerms" : ["bronchitis vs pneumonia"] }', 'OutlineFlyoutInitialShow': 'true', 'PromoBoxContent': '', 'SmartlinksRegionAvailability': '{ "allRegions": true, "regions": ["CAN", "CA", "ca"] }'}, 'state': 'UPDATE', 'templateVersion': '34'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	6/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.RECORD_AUDIO, android.permission.WAKE_LOCK, android.permission.READ_EXTERNAL_STORAGE
Other Common Permissions	2/44	com.android.launcher.permission.INSTALL_SHORTCUT, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

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
www.uptodate.cn	IP: 211.147.88.113 Country: China Region: Shanghai City: Shanghai

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
app.pendo	ok	No Geolocation information available.
jakarta.ee	ok	IP: 52.52.192.191 Country: United States of America Region: California City: San Francisco Latitude: 37.774929 Longitude: -122.419418 View: Google Map

DOMAIN	STATUS	GEOLOCATION
java.sun.com	ok	IP: 23.62.226.2 Country: Japan Region: Tokyo City: Tokyo Latitude: 35.689507 Longitude: 139.691696 View: Google Map
uptodate.com	ok	IP: 199.107.238.205 Country: United States of America Region: California City: San Diego Latitude: 32.894405 Longitude: -117.200951 View: Google Map
www.utdlab.com	ok	No Geolocation information available.
apache.org	ok	IP: 151.101.2.132 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
xml.org	ok	IP: 104.239.142.8 Country: United States of America Region: Texas City: Windcrest Latitude: 29.499678 Longitude: -98.399246 View: Google Map

DOMAIN	STATUS	GEOLOCATION
data.eu.pendo.io	ok	IP: 34.110.214.126 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
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
www.w3.org	ok	IP: 104.18.22.19 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
track.appsflyer.com	ok	IP: 18.155.173.15 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map

DOMAIN	STATUS	GEOLOCATION
github.com	ok	IP: 140.82.113.4 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
survey.qualtrics.com	ok	IP: 23.202.57.104 Country: United States of America Region: California City: San Jose Latitude: 37.339390 Longitude: -121.894958 View: Google Map
www.uptodate.com	ok	IP: 12.130.132.46 Country: United States of America Region: California City: San Diego Latitude: 32.894405 Longitude: -117.200951 View: Google Map
uptodate-5183f.firebaseio.com	ok	IP: 34.120.160.131 Country: United States of America Region: Missouri City: Kansas City Latitude: 39.099731 Longitude: -94.578568 View: Google Map

DOMAIN	STATUS	GEOLOCATION
www.slf4j.org	ok	IP: 159.100.250.151 Country: Switzerland Region: Vaud City: Lausanne Latitude: 46.515999 Longitude: 6.632820 View: Google Map
www.youtube.com	ok	IP: 142.250.74.110 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
data.jpn.pendo.io	ok	IP: 34.149.195.87 Country: United States of America Region: Texas City: Houston Latitude: 29.941401 Longitude: -95.344498 View: Google Map
www.springframework.org	ok	IP: 172.64.151.160 Country: United States of America Region: Texas City: Dallas Latitude: 32.783058 Longitude: -96.806671 View: Google Map

DOMAIN	STATUS	GEOLOCATION
127.0.0.1	ok	IP: 127.0.0.1 Country: - Region: - City: - Latitude: 0.000000 Longitude: 0.000000 View: Google Map
jersey.java.net	ok	IP: 137.254.56.48 Country: United States of America Region: California City: Belmont Latitude: 37.532440 Longitude: -122.248833 View: Google Map
javax.xml.xmlconstants	ok	No Geolocation information available.
www.gstatic.com	ok	IP: 142.250.74.163 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
xml.apache.org	ok	IP: 151.101.2.132 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map

DOMAIN	STATUS	GEOLOCATION
h2database.com	ok	IP: 80.74.147.171 Country: Switzerland Region: Zurich City: Zurich Latitude: 47.366669 Longitude: 8.550000 View: Google Map
events.appsflyer.com	ok	IP: 18.155.173.93 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
jaxb.dev.java.net	ok	IP: 137.254.56.48 Country: United States of America Region: California City: Belmont Latitude: 37.532440 Longitude: -122.248833 View: Google Map
www.wolterskluwer.com	ok	IP: 104.18.35.40 Country: United States of America Region: Texas City: Dallas Latitude: 32.783058 Longitude: -96.806671 View: Google Map
s-s.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
api.appsflyer.com	ok	IP: 18.155.173.74 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
www.uptodate.cn	ok	IP: 211.147.88.113 Country: China Region: Shanghai City: Shanghai Latitude: 31.222219 Longitude: 121.458061 View: Google Map
data.pendo.io	ok	IP: 34.107.204.85 Country: United States of America Region: Missouri City: Kansas City Latitude: 39.099731 Longitude: -94.578568 View: Google Map
ws-i.org	ok	IP: 166.78.156.91 Country: United States of America Region: Illinois City: Chicago Latitude: 41.850029 Longitude: -87.650047 View: Google Map

DOMAIN	STATUS	GEOLOCATION
xmlpull.org	ok	IP: 185.199.110.153 Country: United States of America Region: Pennsylvania City: California Latitude: 40.065632 Longitude: -79.891708 View: Google Map
t.appsflyer.com	ok	IP: 18.155.173.122 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
s.qualtrics.com	ok	IP: 23.202.57.104 Country: United States of America Region: California City: San Jose Latitude: 37.339390 Longitude: -121.894958 View: Google Map
us1.data.pendo.io	ok	IP: 34.110.177.118 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

EMAILS

EMAIL	FILE
xxx@yyy.com	com/uptodate/microservice/content/share/model/ContentShareOfRecipient.java
customerservice@uptodate.com	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Pendo	Analytics	https://reports.exodus-privacy.eu.org/trackers/416
Qualtrics		https://reports.exodus-privacy.eu.org/trackers/306

HARDCODED SECRETS

POSSIBLE SECRETS
"com.google.firebase.crashlytics.mapping_file_id" : "b94a23daaa0a4571a25f288fb1121585"
"firebase_database_url" : "https://uptodate-5183f.firebaseio.com"
"google_api_key" : "AlzaSyC2HGA1oOlho-k9RIHlrq-bnBOL5II2Ge4"
"google_crash_reporting_api_key" : "AlzaSyC2HGA1oOlho-k9RIHlrq-bnBOL5II2Ge4"
"password" : "Password"
"password" : "□□□□□"
"share_success_guest_pass" : "□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□"
"user_name" : "□□□□□"
"password" : "Passwort"
"user_name" : "Benutzername"
"password" : "□□"
"user_name" : "□□□"
"password" : "Wachtwoord"
"user_name" : "Gebruikersnaam"
"password" : "Hasło"

POSSIBLE SECRETS
"password" : "██"
"password" : "Parola"
"password" : "Contraseña"
"password" : "Password"
"password" : "Palavra-passe"
"password" : "Пароль"
"password" : "██"
"share_success_guest_pass" : "██████████████████████████████████████"
"user_name" : "██████"
"password" : "██"
"share_success_guest_pass" : "██████████████████████████████████████"
"user_name" : "████"
"password" : "██"
"share_success_guest_pass" : "██████████████████████████████████████"
"user_name" : "██████"

POSSIBLE SECRETS

FFFFFFFFFFFFFFFFC90FDA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64ECFB850458DBEF0A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D2261AD2EE6BF12FFA06D98A0864D87602733EC86A64521F2B18177B200CBBE117577A615D6C770988C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A93AD2CAFFFFFFFFFFFFFFFF

MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC1B6qsa2sbpc4CuFEjgRWez9nN

FFFFFFFFFFFFFFFFC90FDA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64ECFB850458DBEF0A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D2261AD2EE6BF12FFA06D98A0864D87602733EC86A64521F2B18177B200CBBE117577A615D6C770988C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A92108011A723C12A787E6D788719A10BDBA5B2699C327186AF4E23C1A946834B6150BDA2583E9CA2AD44CE8DBBBC2DB04DE8EF92E8EFC141FBECAA6287C59474E6BC05D99B2964FA090C3A2233BA186515BE7ED1F612970CEE2D7AFB81BDD762170481CD0069127D5B05AA993B4EA988D8FDDC186FFB7DC90A6C08F4DF435C93402849236C3FAB4D27C7026C1D4DCB2602646DEC9751E763DBA37BDF8FF9406AD9E530EE5DB382F413001AEB06A53ED9027D831179727B0865A8918DA3EDBEBBCF9B14ED44CE6CBACED4BB1BDB7F1447E6CC254B332051512BD7AF426FB8F401378CD2BF5983CA01C64B92ECF032EA15D1721D03F482D7CE6E74FEF6D55E702F46980C82B5A84031900B1C9E59E7C97FBEC7E8F323A97A7E36CC88BE0F1D45B7FF585AC54BD407B22B4154AAC8F6D7EBF48E1D814CC5ED20F8037E0A79715EEF29BE32806A1D58BB7C5DA76F550AA3D8A1FBFF0EB19CCB1A313D55CDA56C9EC2EF29632387FE8D76E3C0468043E8F663F4860EE12BF2D5B0B7474D6E694F91E6DCC4024FFFFFFFFFFFFFFFF

41058363725152142129326129780047268409114441015993725554835256314039467401291

FFFFFFFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3DF1ED5D5FD65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB182B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9CE98583FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFFA886B4238611FCFDCDE355B3B6519035BBC34F4DEF99C023861B46FC9D6E6C9077AD91D2691F7F7EE598CB0FAC186D91CAEFE130985139270B4130C93BC437944F4FD4452E2D74DD364F2E21E71F54BFF5CAE82AB9C9DF69EE86D2BC522363A0DABC521979B0DEADA1DBF9A42D5C4484E0ABCD06BFA53DDEF3C1B20EE3FD59D7C25E41D2B66C62E37FFFFFFFFFFFFFFFF

fd7f53811d75122952df4a9c2eece4e7f611b7523cef4400c31e3f80b6512669455d402251fb593d8d58fabfc5f5ba30f6cb9b556cd7813b801d346ff26660b76b9950a5a49f9fe8047b1022c24fbba9d7feb7c61bf83b57e7c6a8a6150f04fb83f6d3c51ec3023554135a169132f675f3ae2b61d72aeff22203199dd14801c7

POSSIBLE SECRETS
VTdL1VbC2tejvcl2BIMkEpk1BzBZI0KQB0GaDWFLN
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8ACAA68FFFFFFFFFFFFFFFF
Vd99BKh6pxt3mXSDJzHuVrCq52xBXAKVahbuFb6dqBc
32670510020758816978083085130507043184471273380659243275938904335757337482424
nvknbo5+6pBVWVZpCg5Rtpii3JUKMxOmJrccBCo7IClqPIj/L9Nc5zmWMH2igKHLq
95475cf5d93e596c3fcd1d902add02f427f5f3c7210313bb45fb4d5bb2e5fe1cbd678cd4bddd84c9836be1f31c0777725aeb6c2fc38b85f48076fa76bcd8146cc89a6fb2f706dd719898c2083dc8d896f84062e2c9c94d137b054a8d8096adb8d51952398eeca852a0af12df83e475aa65d4ec0c38a9560d5661186ff98b9fc9eb60eee8b030376b236bc73be3acdbd74fd61c1d2475fa3077b8f080467881ff7e1ca56fee066d79506ade51edbb5443a563927dbc4ba520086746175c8885925ebc64c6147906773496990cb714ec667304e261faee33b3cbdf008e0c3fa90650d97d3909c9275bf4ac86ffc3d03e6dfc8ada5934242dd6d3bcc2a406cb0b
7AEIOUY8HW1BFPV2CGJKQ5XZ3DT4L5MN6R
FFFFFFFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3DF1ED5D5FD65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB182B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9CE98583FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFFA886B423861285C97FFFFFFFFFFFFFFFF
55066263022277343669578718895168534326250603453777594175500187360389116729240
046b6c7f-0b8a-43b9-b35d-6489e6daee92
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE65381FFFFFFFFFFFFFFFF

POSSIBLE SECRETS

FFFFFFFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3D
F1ED5D5FD65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB1
82B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9C
E98583FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFA886B4238611FCFDCDE355B3B6519035BBC34F4DEF99
C023861B46FC9D6E6C9077AD91D2691F7F7EE598CB0FAC186D91CAEFE130985139270B4130C93BC437944F4FD4452E2D74DD364F2E21E71F54BFF5CAE82AB9C9DF6
9EE86D2BC522363A0DABC521979B0DEADA1DBF9A42D5C4484E0ABCD06BFA53DDEF3C1B20EE3FD59D7C25E41D2B669E1EF16E6F52C3164DF4FB7930E9E4E58857B
6AC7D5F42D69F6D187763CF1D5503400487F55BA57E31CC7A7135C886EFB4318AED6A1E012D9E6832A907600A918130C46DC778F971AD0038092999A333CB8B7A1
A1DB93D7140003C2A4ECEA9F98D0ACC0A8291CDCEC97DCF8EC9B55A7F88A46B4DB5A851F44182E1C68A007E5E0DD9020BFD64B645036C7A4E677D2C38532A3A23
BA4442CAF53EA63BB454329B7624C8917BDD64B1C0FD4CB38E8C334C701C3ACDAD0657FCCFEC719B1F5C3E4E46041F388147FB4CFDB477A52471F7A9A96910B855
322EDB6340D8A00EF092350511E30ABEC1FFF9E3A26E7FB29F8C183023C3587E38DA0077D9B4763E4E4B94B2BBC194C6651E77CAF992EEAAC0232A281BF6B3A739C
1226116820AE8DB5847A67CBEF9C9091B462D538CD72B03746AE77F5E62292C311562A846505DC82DB854338AE49F5235C95B91178CCF2DD5CACEF403EC9D1810C
6272B045B3B71F9DC6B80D63FDD4A8E9ADB1E6962A69526D43161C1A41D570D7938DAD4A40E329CCFF46AAA36AD004CF600C8381E425A31D951AE64FDB23FCEC
9509D43687FEB69EDD1CC5E0B8CC3BDF64B10EF86B63142A3AB8829555B2F747C932665CB2C0F1CC01BD70229388839D2AF05E454504AC78B7582822846C0BA35C
35F5C59160CC046FD8251541FC68C9C86B022BB7099876A460E7451A8A93109703FEE1C217E6C3826E52C51AA691E0E423CFC99E9E31650C1217B624816CDAD9A95
F9D5B8019488D9C0A0A1FE3075A577E23183F81D4A3F2FA4571EFC8CE0BA8A4FE8B6855DFE72B0A66EDED2FBABFBE58A30FAFABE1C5D71A87E2F741EF8C1FE86FEA
6BBFDE530677F0D97D11D49F7A8443D0822E506A9F4614E011E2A94838FF88CD68C8BB7C5C6424CFFFFFFFFFFFFFFFFF

046b6c7f-0b8a-43b9-b35d-6489e6daee91

115792089237316195423570985008687907852837564279074904382605163141518161494337

39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319

115792089210356248762697446949407573530086143415290314195533631308867097853951

01360240043788015936020505

26617408020502170632287687167233609607298591687569731477066713684188029449964278084915450806277719023520942412250655586621571135455709
16814161637315895999846

68647976601306097149819007990813932172694353001433054093944634591855431833976553942450577463332171975329639963713633211138647686124403
80340372808892707005449

POSSIBLE SECRETS

POSSIBLE SECRETS
AC6BDB41324A9A9BF166DE5E1389582FAF72B6651987EE07FC3192943DB56050A37329CBB4A099ED8193E0757767A13DD52312AB4B03310DCD7F48A9DA04FD50E8083969EDB767B0CF6095179A163AB3661A05FBD5FAAAE82918A9962F0B93B855F97993EC975EEAA80D740ADBFF4FF747359D041D5C33EA71D281E446B14773BCA97B43A23FB801676BD207A436C6481F1D2B9078717461A5B9D32E688F87748544523B524B0D57D5EA77A2775D2ECFA032CFBDBF52FB3786160279004E57AE6AF874E7303CE53299CCC041C7BC308D82A5698F3A8D0C38271AE35F8E9DBFBB694B5C803D89F7AE435DE236D525F54759B65E372FCD68EF20FA7111F9E4AFF73
39402006196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643
1093849038073734274511112390766805569936207598951683748994586394495953116150735016013708737573759623248592132296706313309438452531591012912142327488478985984
3757180025770020463545507224491183603594455134769762486694567779615544477440556316691234405012945539562144444537289428522585666729196580810124344277578376784
EEAF0AB9ADB38DD69C33F80AFA8FC5E86072618775FF3C0B9EA2314C9C256576D674DF7496EA81D3383B4813D692C6E0E0D5D8E250B98BE48E495C1D6089DAD15DC7D7B46154D6B6CE8EF4AD69B15D4982559B297BCF1885C529F566660E57EC68EDBC3C05726CC02FD4CBF4976EAA9AFD5138FE8376435B9FC61D2FC0EB06E3
dc12a687-737f-11cf-884d-00aa004b2e24
f7e1a085d69b3ddecbcab5c36b857b97994afbbfa3aea82f9574c0b3d0782675159578ebad4594fe67107108180b449167123e84c281613b7cf09328cc8a6e13c167a8b547c8d28e0a3ae1e2bb3a675916ea37f0bfa213562f1fb627a01243bcca4f1bea8519089a883dfe15ae59f06928b665e807b552564014c3bfecf492a
50A7E9B0-70EF-11D1-B75A-00A0C90564FE
53F56307-B6BF-11D0-94F2-00A0C91EFB8B
962eddcc369cba8ebb260ee6b6a126d9346e38c5

POSSIBLE SECRETS
FFFFFFFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3D F1ED5D5FD65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB1 82B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9C E98583FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFA886B4238611FCFDCDE355B3B6519035BBC34F4DEF99 C023861B46FC9D6E6C9077AD91D2691F7F7EE598CB0FAC186D91CAEFE130985139270B4130C93BC437944F4FD4452E2D74DD364F2E21E71F54BFF5CAE82AB9C9DF6 9EE86D2BC522363A0DABC521979B0DEADA1DBF9A42D5C4484E0ABCD06BFA53DDEF3C1B20EE3FD59D7C25E41D2B669E1EF16E6F52C3164DF4FB7930E9E4E58857B 6AC7D5F42D69F6D187763CF1D5503400487F55BA57E31CC7A7135C886EFB4318AED6A1E012D9E6832A907600A918130C46DC778F971AD0038092999A333CB8B7A1 A1DB93D7140003C2A4ECEA9F98D0ACC0A8291CDCEC97DCF8EC9B55A7F88A46B4DB5A851F44182E1C68A007E5E655F6AFFFFFFFFFFFFFFFFF
115792089210356248762697446949407573530086143415290314195533631308867097853948
GuyRRmX3DYoWdTvGeN3u0gJw5MsXul9K7yDiO
FFFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1 356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA483 61C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA237327FFFFFFFFFFFFFFFFF
115792089237316195423570985008687907853269984665640564039457584007908834671663
fca682ce8e12caba26efccf7110e526db078b05edecbcd1eb4a208f3ae1617ae01f35b91a47e6df63413c5e12ed0899bcd132acd50d99151bdc43ee737592e17
27580193559959705877849011840389048093056905856361568521428707301988689241309860865136260764883745107765439761230575
4590f811-1d3a-11d0-891f-00aa004b2e24
470fa2b4ae81cd56ecbcd9735803434cec591fa
678471b27a9cf44ee91a49c5147db1a9aaf244f05a434d6486931d2d14271b9e35030b71fd73da179069b32e2935630e1c2062354d0da20a6c416e50be794ca4
86E0D1E0-8089-11D0-9CE4-08003E301F73
nMcadFr9rxwGUMGOn8qlcjLE4vr9T1rxm6DekW9IBGNAwGOynuA+ebTfpPMYY8nO

POSSIBLE SECRETS
FFFFFFFFFFFFFFFFC90FDA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64ECFB850458DBEF0A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D2261AD2EE6BF12FFA06D98A0864D87602733EC86A64521F2B18177B200CBBE117577A615D6C770988C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A92108011A723C12A787E6D788719A10BD8A5B2699C327186AF4E23C1A946834B6150BDA2583E9CA2AD44CE8DBBCC2DB04DE8EF92E8EFC141FBECAA6287C59474E6BC05D99B2964FA090C3A2233BA186515BE7ED1F612970CEE2D7AFB81BDD762170481CD0069127D5B05AA993B4EA988D8FDDC186FFB7DC90A6C08F4DF435C934063199FFFFFFFFFFFFFFFF
b869c82b35d70e1b1ff91b28e37a62ecdc34409b
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057148
42debb9da5b3d88cc956e08787ec3f3a09bba5f48b889a74aaf53174aa0fbe7e3c5b8fcd7a53bef563b0e98560328960a9517f4014d3325fc7962bf1e049370d76d1314a76137e792f3f0db859d095e4a5b932024f079ecf2ef09c797452b0770e1350782ed57ddf794979dcef23cb96f183061965c4ebc93c9c71c56b925955a75f94ccc1449ac43d586d0beee43251b0b2287349d68de0d144403f13e802f4146d882e057af19b6f6275c6676c8fa0e3ca2713a3257fd1b27d0639f695e347d8d1cf9ac819a26ca9b04cb0eb9b7b035988d15bbac65212a55239cfc7e58fae38d7250ab9991ffb9c97134025fe8ce04c4399ad96569be91a546f4978693c7a
3082018b3081f502044295ce6b300d06092a864886f70d0101040500300d310b3009060355040313024832301e170d3035303532363133323630335a170d3337303933303036353734375a300d310b300906035504031302483230819f300d06092a864886f70d010101050003818d0030818902818100dc0a13c602b7141110eade2f051b54777b060d0f74e6a110f9cce81159f271ebc88d8e8aa1f743b505fc2e7dfe38d33b8d3f64d1b363d1af4d877833897954cbaec2fa384c22a415498cf306bb07ac09b76b001cd68bf77ea0a628f5101959cf2993a9c23dbee79b19305977f8715ae78d023471194cc900b231eecb0aaea98d0203010001300d06092a864886f70d01010405000381810083f4401a279453701bef9a7681a5b8b24f153f7d18c7c892133d97bd5f13736be7505290a445a7d5ceb75522403e5097515cd966ded6351ff60d5193de34cd36e5cb04d380398e66286f99923fd92296645fd4ada45844d194dfd815e6cd57f385c117be982809028bba1116c85740b3d27a55b1a0948bf291ddba44bed337b9
sXchDaQebHnPiGvyDOAT4saGEUetSyo9MKLOoWFsueri23bOdgWp4Dy1WlUzewbgBHod5pcM9H95GQVR3JDXboIRROSBigeC5yjU1hGzHHyXss8UDprecbaYxknTcQkhsIANGRUZmdTOQ5qTRsLat6BTYuyvVRdhS8exSZEy
B196B286-BAB4-101A-B69C-00AA00341D07
FDB497E7C6F9D71A89D042B0FA5B7A4DEA5EE7938F08CFDA9F1FB58EBDF749E7

POSSIBLE SECRETS
48439561293906451759052585252797914202762949526041747995844080717082404635286
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112316
B196B284-BAB4-101A-B69C-00AA00341D07
b0b4417601b59cbc9d8ac8f935cadaec4f5fbb2f23785609ae466748d9b5a536
9760508f15230bccb292b982a2eb840bf0581cf5
e9e642599d355f37c97ffd3567120b8e25c9cd43e927b3a9670fbec5d890141922d2c3b3ad2480093799869d1e846aab49fab0ad26d2ce6a22219d470bce7d777d4a21fbe9c270b57f607002f3cef8393694cf45ee3688c11a8c56ab127a3daf
36134250956749795798585127919587881956611106672985015071877198253568414405109
9DEF3CAFB939277AB1F12A8617A47BBBDBA51DF499AC4C80BEEEA9614B19CC4D5F4F5F556E27CBDE51C6A94BE4607A291558903BA0D0F84380B655BB9A22E8DCD F028A7CEC67F0D08134B1C8B97989149B609E0BE3BAB63D47548381DBC5B1FC764E3F4B53DD9DA1158BFD3E2B9C8CF56EDF019539349627DB2FD53D24B7C48665 772E437D6C7F8CE442734AF7CCB7AE837C264AE3A9BEB87F8A2FE9B8B5292E5A021FFF5E91479E8CE7A28C2442C6F315180F93499A234DCF76E3FED135F9BB
77d0f8c4dad15eb8c4f2f8d6726cefd96d5bb399
44aca674-e8fc-11d0-a07c-00c04fb68820
23456789abcdefghijklmnopqrstuvwxyz
68647976601306097149819007990813932172694353001433054093944634591855431833976560521225596406614545549772963113914808580371219879997166 43812574028291115057151
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1 356D6D51C245E485B576625E7EC6F44C42E9A63A3620FFFFFFFFFFFFFFFF

POSSIBLE SECRETS
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCbelsiqvdpzGmRF3pex4Ar1HNI
f8183668ba5fc5bb06b5981e6d8b795d30b8978d43ca0ec572e37e09939a9773
Ct4eTIXHBIY2EaV7t7LjjaynVJCpkv4LKjTTAumiGUluQhrNhZLuF
30820277020100300d06092a864886f70d0101010500048202613082025d02010002818100dc0a13c602b7141110eade2f051b54777b060d0f74e6a110f9cce81159f271ebc88d8e8aa1f743b505fc2e7dfe38d33b8d3f64d1b363d1af4d877833897954cbaec2fa384c22a415498cf306bb07ac09b76b001cd68bf77ea0a628f5101959cf2993a9c23dbee79b19305977f8715ae78d023471194cc900b231eecb0aeea98d02030100010281810099aa4ff4d0a09a5af0bd953cb10c4d08c3d98df565664ac5582e494314d5c3c92dddedd5d316a32a206be4ec084616fe57be15e27cad111aa3c21fa79e32258c6ca8430afc69eddd52d3b751b37da6b6860910b94653192c0db1d02abcf6ce14c01f238eec7c20bd3bb750940004bacba2880349a9494d10e139ecb2355d101024100ffdc3defd9c05a2d377ef6019fa62b3bfd5b0020a04cc8533bca730e1f6fcf5dfceea1b044fbe17d9eababfbc7d955edad6bc60f9be826ad2c22ba77d19a9f65024100dc28d43fdbbc93852cc3567093157702bc16f156f709fb7db0d9eec028f41fd0edcd17224c866e66be1744141fb724a10fd741c8a96afdd9141b36d67fff6309024077b1cddbde0f69604bdcfe33263fb36ddf24aa3b9922327915b890f8a36648295d0139ecdf68c245652c4489c6257b58744fbdd961834a4cab201801a3b1e52d024100b17142e8991d1b350a0802624759d48ae2b8071a158ff91fabeb6a8f7c328e762143dc726b8529f42b1fab6220d1c676fdc27ba5d44e847c72c52064afd351a902407c6e23fe35bcfcd1a662aa82a2aa725fcede311644d5b6e3894853fd4ce9fe78218c957b1ff03fc9e5ef8ffeb6bd58235f6a215c97d354fdace7e781e4a63e8b
57896044618658097711785492504343953926634992332820282019728792003956564819949
8d5155894229d5e689ee01e6018a237e2cae64cd
726838724295606890549323807888004534353641360687318060281490199180612328166730772686396383698676545930088884461843637361053498018365439
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCv8lqRRwpH8s7EnWhLwuFqnbTA
674B6698-EE92-11D0-AD71-00C04FD8FDFF

POSSIBLE SECRETS
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B5766257EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64ECFB850458DBEF0A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D2261AD2EE6BF12FFA06D98A0864D87602733EC86A64521F2B18177B200CBBE117577A615D6C770988C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A92108011A723C12A787E6D788719A10BD8A5B2699C327186AF4E23C1A946834B6150BDA2583E9CA2AD44CE8DBBBC2DB04DE8EF92E8EFC141FBECAA6287C59474E6BC05D99B2964FA090C3A2233BA186515BE7ED1F612970CEE2D7AFB81BDD762170481CD0069127D5B05AA993B4EA988D8FDDC186FFB7DC90A6C08F4DF435C93402849236C3FAB4D27C7026C1D4DCB2602646DEC9751E763DBA37BDF8FF9406AD9E530EE5DB382F413001AEB06A53ED9027D831179727B0865A8918DA3EDBEBCF9B14ED44CE6CBACED4BB1BDB7F1447E6CC254B332051512BD7AF426FB8F401378CD2BF5983CA01C64B92ECF032EA15D1721D03F482D7CE6E74FEF6D55E702F46980C82B5A84031900B1C9E59E7C97FBEC7E8F323A97A7E36CC88BE0F1D45B7FF585AC54BD407B22B4154AAC8F6D7EBF48E1D814CC5ED20F8037E0A79715EEF29BE32806A1D58BB7C5DA76F550AA3D8A1FBFF0EB19CCB1A313D55CDA56C9EC2EF29632387FE8D76E3C0468043E8F663F4860EE12BF2D5B0B7474D6E694F91E6DBE115974A3926F12FEE5E438777CB6A932DF8CD8BEC4D073B931BA3BC832B68D9DD300741FA7BF8AFC47ED2576F6936BA424663AAB639C5AE4F5683423B4742BF1C978238F16CBE39D652DE3FDB8BEFC848AD92222E04A4037C0713EB57A81A23F0C73473FC646CEA306B4BCBC8862F8385DDFA9D4B7FA2C087E879683303ED5BDD3A062B3CF5B3A278A66D2A13F83F44F82DDF310EE074AB6A364597E899A0255DC164F31CC50846851DF9AB48195DED7EA1B1D510BD7EE74D73FAF36BC31ECFA268359046F4EB879F924009438B481C6CD7889A002ED5EE382BC9190DA6FC026E479558E4475677E9AA9E3050E2765694DFC81F56E880B96E7160C980DD98EDD3DFFFFFFFFFFFFFFFFF
26247035095799689268623156744566981891852923491109213387815615900925518854738050089022388053975719786650872476732087
983af869-c0f9-4bac-b645-b9ea20043235

PLAYSTORE INFORMATION

Title: UpToDate

Score: 4.51 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.uptodate.android

Developer Details: Wolters Kluwer Health UpToDate, Wolters+Kluwer+Health+UpToDate, None, <http://www.uptodate.com/home/uptodate-mobile-access>, support@uptodate.com,

Release Date: May 9, 2012 **Privacy Policy:** [Privacy link](#)

Description:

Individual or Institutional Subscription required. UpToDate® registrants and Individual subscribers can now answer their clinical questions anytime, anywhere by

downloading this app onto an Android™ phone or tablet. UpToDate is the leading clinical decision support resource with evidence-based clinical information – including drug topics and recommendations that clinicians rely on at the point of care. UpToDate has been the subject of over 30 research studies confirming that widespread usage of UpToDate is associated with improved patient care and hospital performance. UpToDate for Android Features: • Persistent login • Easy search with auto-completion • Earn and track free CME/CE/CPD credit • Bookmarks and history • Mobile-optimized medical calculators • Email topics and graphics to patients and colleagues We would love to hear your feedback. Please contact us with questions or feedback at customerservice@uptodate.com. Thank you! Permissions the UpToDate app requires and how it uses them: • Network communications: used to download and update content from UpToDate. • Permissions to store UpToDate Content/app preferences in the internal storage or external storage(SD Card).

SCAN LOGS

Timestamp	Event	Error
2025-09-01 11:04:12	Generating Hashes	OK
2025-09-01 11:04:12	Extracting APK	OK
2025-09-01 11:04:12	Unzipping	OK
2025-09-01 11:04:12	Parsing APK with androguard	OK
2025-09-01 11:04:13	Extracting APK features using aapt/aapt2	OK
2025-09-01 11:04:13	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 11:04:16	Parsing AndroidManifest.xml	OK

2025-09-01 11:04:16	Extracting Manifest Data	OK
2025-09-01 11:04:16	Manifest Analysis Started	OK
2025-09-01 11:04:16	Performing Static Analysis on: UpToDate (com.uptodate.android)	OK
2025-09-01 11:04:17	Fetching Details from Play Store: com.uptodate.android	OK
2025-09-01 11:04:19	Checking for Malware Permissions	OK
2025-09-01 11:04:19	Fetching icon path	OK
2025-09-01 11:04:19	Library Binary Analysis Started	OK
2025-09-01 11:04:19	Reading Code Signing Certificate	OK
2025-09-01 11:04:19	Running APKiD 2.1.5	OK
2025-09-01 11:04:22	Detecting Trackers	OK
2025-09-01 11:04:26	Decompiling APK to Java with JADX	OK

2025-09-01 11:04:47	Decompiling with JADX failed, attempting on all DEX files	OK
2025-09-01 11:04:47	Decompiling classes2.dex with JADX	OK
2025-09-01 11:04:55	Decompiling classes4.dex with JADX	OK
2025-09-01 11:05:03	Decompiling classes.dex with JADX	OK
2025-09-01 11:05:12	Decompiling classes3.dex with JADX	OK
2025-09-01 11:05:20	Decompiling classes2.dex with JADX	OK
2025-09-01 11:05:29	Decompiling classes4.dex with JADX	OK
2025-09-01 11:05:36	Decompiling classes.dex with JADX	OK
2025-09-01 11:05:45	Decompiling classes3.dex with JADX	OK
2025-09-01 11:05:53	Converting DEX to Smali	OK
2025-09-01 11:05:53	Code Analysis Started on - java_source	OK

2025-09-01 11:06:00	Android SBOM Analysis Completed	OK
2025-09-01 11:06:11	Android SAST Completed	OK
2025-09-01 11:06:11	Android API Analysis Started	OK
2025-09-01 11:06:23	Android API Analysis Completed	OK
2025-09-01 11:06:23	Android Permission Mapping Started	OK
2025-09-01 11:06:31	Android Permission Mapping Completed	OK
2025-09-01 11:06:32	Android Behaviour Analysis Started	OK
2025-09-01 11:06:45	Android Behaviour Analysis Completed	OK
2025-09-01 11:06:45	Extracting Emails and URLs from Source Code	OK
2025-09-01 11:06:52	Email and URL Extraction Completed	OK
2025-09-01 11:06:52	Extracting String data from APK	OK

2025-09-01 11:06:52	Extracting String data from Code	OK
2025-09-01 11:06:52	Extracting String values and entropies from Code	OK
2025-09-01 11:06:57	Performing Malware check on extracted domains	OK
2025-09-01 11:07:05	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.

© 2025 Mobile Security Framework - MobSF | [Ajin Abraham](#) | [OpenSecurity](#).