ANDROID STATIC ANALYSIS REPORT

Contour (3.5.0)

File Name:	com.ascensia.contour.us_13130.apk
Package Name:	com.ascensia.contour.us
Scan Date:	Aug. 29, 2025, 7:56 p.m.
App Security Score:	64/100 (LOW RISK)
Grade:	A
Trackers Detection:	3/432

FINDINGS SEVERITY

HIGH	⚠ MEDIUM	INFO	✓ SECURE	HOTSPOT
4	17	1	9	1

FILE INFORMATION

File Name: com.ascensia.contour.us_13130.apk
Size: 29.08MB
MD5: f1dcc9ee377147a50f8c9ab4b4b1dec9
SHA1: 197a4fcd87facb979c1597e8944a5e0b2fe191eb
SHA256: a33eb9c86f438c60e0dbdb9b9c2489050a75483370555f2ef56e8a52c5142fc4

APP INFORMATION

App Name: Contour
Package Name: com.ascensia.contour.us
Main Activity: com.ascensia.contour.MainActivity
Target SDK: 34
Min SDK: 21
Max SDK:
Android Version Name: 3.5.0

Android Version Code: 13130

APP COMPONENTS

Activities: 18
Services: 16
Receivers: 16
Providers: 3
Exported Activities: 0
Exported Services: 2
Exported Receivers: 3
Exported Providers: 0

CERTIFICATE INFORMATION

```
Binary is signed
v1 signature: True
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=us, ST=newyork, L=tarrytown, O=ascensia diabetes care, OU=diabetes, CN=ascensia diabetes
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2015-12-18 17:50:41+00:00
Valid To: 4753-11-14 17:50:41+00:00
Issuer: C=us, ST=newyork, L=tarrytown, O=ascensia diabetes care, OU=diabetes, CN=ascensia diabetes
Serial Number: 0x1a0455ea
Hash Algorithm: sha256
md5: 3338b28ffcf3032bb46a3de7721d2cda
sha1: 1d5bcf5ed37d4cf8bf2eb42972fd34dba1b1faa9
sha256: db343477768ac1d19fa630784458bba5c227653cb4d6e2163f70424b29d02e8d
sha512: 329af4d240efdd1e2a7e242458034b426c9e14ae4e1518949a5c78047894af66d326e2e7cc91ee895ba12e86a8d16265b811880eafe4cf063f98c92e73899fb3
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: f830c20f73b5be68c93c0bbfa1d549311af3ec75523ea9d8f60e8d56de15b845
Found 1 unique certificates
```

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WRITE_INTERNAL_STORAGE	unknown	Unknown permission	Unknown permission from android reference
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
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.BLUETOOTH_SCAN	dangerous	required for discovering and pairing Bluetooth devices.	Required to be able to discover and pair nearby Bluetooth devices.
android.permission.BLUETOOTH_ADVERTISE	dangerous	required to advertise to nearby Bluetooth devices.	Required to be able to advertise to 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.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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.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.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference
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.
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.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.SCHEDULE_EXACT_ALARM	normal	permits exact alarm scheduling for background work.	Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.
android.permission.READ_MEDIA_IMAGES	dangerous	allows reading image files from external storage.	Allows an application to read image files from external storage.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.USE_EXACT_ALARM	normal	allows using exact alarms without user permission.	Allows apps to use exact alarms just like with SCHEDULE_EXACT_ALARM but without needing to request this permission from the user. This is only intended for use by apps that rely on exact alarms for their core functionality. You should continue using SCHEDULE_EXACT_ALARM if your app needs exact alarms for a secondary feature that users may or may not use within your app. Keep in mind that this is a powerful permission and app stores may enforce policies to audit and review the use of this permission. Such audits may involve removal from the app store if the app is found to be misusing this permission.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
com.ascensia.contour.us.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check
Build.BRAND check
Build.DEVICE check
Build.TAGS check
SIM operator check
network operator name check</td></tr>
<tr><td>Compiler</td><td>dx</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.ascensia.contour.MainActivity	Schemes: onyx://, Path Prefixes: Contourapp,

NETWORK SECURITY

HIGH: **0** | WARNING: **0** | INFO: **0** | SECURE: **7**

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	secure	Base config is configured to disallow clear text traffic to all domains.

NO	SCOPE	SEVERITY	DESCRIPTION
2	contourstagingcloud.ascensia.com	secure	Certificate pinning does not have an expiry. Ensure that pins are updated before certificate expire. [Pin: ZqtDjEa7ac/tHB7uuIQ0byQkG+mVsJBwlcQafd4lHVM= Digest: SHA-256]
3	contourcloudrussia.ascensia.com	secure	Certificate pinning does not have an expiry. Ensure that pins are updated before certificate expire. [Pin: f6Ml+488FHONcAl0TGR4pzwO4ejqEHaK3q0lyYL12Ag= Digest: SHA-256]
4	contourcloudasia.ascensia.com	secure	Certificate pinning does not have an expiry. Ensure that pins are updated before certificate expire. [Pin: pY3xANZJpY/c1suQk8ehNMNCVzfEtGOPutA550/ng1c= Digest: SHA-256]
5	contourcloudus.ascensia.com	secure	Certificate pinning does not have an expiry. Ensure that pins are updated before certificate expire. [Pin: izgxwotGR0fC/dUS0OqUeRCU5D0eWUAcPdR5lyWAbmw= Digest: SHA-256]
6	contourcloudeu.ascensia.com	secure	Certificate pinning does not have an expiry. Ensure that pins are updated before certificate expire. [Pin: a9zxfAOzAGd+BEL/P3NGzN5b5b/S214R56ZOIa6tW0o= Digest: SHA-256]
7	contourcloudazuredev.ascensia.com	secure	Certificate pinning does not have an expiry. Ensure that pins are updated before certificate expire. [Pin: 59FwFQCcDIsybqnBSYUqxJQqzpkzp/wbXHYQTjeMdYY= Digest: SHA-256]

CERTIFICATE ANALYSIS

HIGH: **0** | WARNING: **1** | INFO: **1**

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.

MANIFEST ANALYSIS

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

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 5.0-5.0.2, [minSdk=21]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.
3	Service (com.ascensia.contour.BleService) is not Protected. [android:exported=true]	warning	A Service 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.

NO	ISSUE	SEVERITY	DESCRIPTION
5	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service 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.
6	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) 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.
7	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: **3** | WARNING: **9** | INFO: **1** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a0/c.java a1/e0.java a2/h.java a2/i.java a2/k.java a2/q.java a2/z.java b2/i.java b2/j.java b3/a.java c1/i.java c2/e.java c2/i.java com/ascensia/contour/CountryCodePicker.java com/ascensia/contour/EnableMFA.java com/ascensia/contour/FirebaseService.java com/ascensia/contour/InternalWebActivity.java com/ascensia/contour/MainActivity.java com/ascensia/contour/PopupWebview.java com/ascensia/contour/RegistrationIntentService.java com/ascensia/contour/SnaqDetailsActivity.java com/ascensia/contour/VerifyOTP.java com/bumptech/glide/b.java com/bumptech/glide/load/data/b.java com/bumptech/glide/load/data/j.java com/bumptech/glide/load/data/l.java com/bumptech/glide/manager/e.java com/bumptech/glide/manager/p.java com/bumptech/glide/manager/q.java com/jeremyfeinstein/slidingmenu/lib/S

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	lidingMenu.java com/jeremyfeinstein/slidingmenu/lib/b.java com/microsoft/windowsazure/messaging/notificationhubs/e.java com/samsung/android/sdk/healthdata/HealthDataObserver.java com/samsung/android/sdk/healthdata/HealthDataStore.java com/samsung/android/sdk/healthdata/HealthPermissionManager.java com/samsung/android/sdk/internal/database/BulkCursorToCursorAdaptor.java com/samsung/android/sdk/internal/healthdata/DeviceUtil.java com/samsung/android/sdk/internal/healthdata/HealthResultHolderImpl.java com/samsung/android/sdk/internal/healthdata/StreamUtil.java d2/a.java d4/o.java d5/d.java e2/c.java e2/d.java e2/g.java e2/t.java e2/u.java e2/v.java e4/t.java e5/b.java f0/a.java g2/a.java g5/g.java g6/b.java h2/b0.java h2/c.java h2/d.java h2/k.java h2/m.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
			OWASP MASVS: MSTG-STORAGE-3	h2/n.java h2/r.java h2/z.java h6/c.java j0/a.java j3/a.java j3/d.java j7/a.java j7/f.java l1/n.java l2/a.java l2/d.java l2/j.java l4/a.java m/d.java m1/d.java m3/b.java m3/d.java m3/e.java m3/i.java m3/j.java m3/s.java m3/u.java m3/v.java m4/a.java n2/d.java n3/d0.java n3/e.java n3/i.java n3/i0.java n3/j.java n3/u.java n3/y.java o0/b.java p/f.java p2/i.java p3/t.java p4/h.java q0/k0.java q0/o.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				q0/o0.java q0/r.java q2/i.java q3/a.java q3/c.java q3/c1.java q3/f1.java q3/p0.java q3/s0.java q3/t0.java q3/u0.java q3/w.java q3/w0.java q3/x.java q8/g.java r/a.java r5/e.java s0/a.java s1/i.java t3/a.java u0/h.java u2/a.java u3/f.java u3/n.java u3/o.java u5/g.java u5/o.java v0/d.java w/c.java w0/a.java w1/a.java x1/d.java x1/e.java y3/b.java z0/a.java z1/c.java z1/e.java z2/k.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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	f3/b0.java f3/f0.java f3/h0.java l7/a.java v0/c.java
3	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/ascensia/contour/MainActivity.java r1/b.java
4	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/ascensia/contour/InternalWebActivity.java com/ascensia/contour/MainActivity.java com/ascensia/contour/PopupWebview.java
5	Ensure that user controlled URLs never reaches the Webview. Enabling file access from URLs in WebView can leak sensitive information from the file system.	warning	CWE: CWE-200: Information Exposure OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	com/ascensia/contour/MainActivity.java
6	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/ascensia/contour/MainActivity.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	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	d8/a.java d8/b.java e7/f.java e8/a.java j7/h.java
8	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	a2/d.java a2/p.java a2/x.java h1/d.java s1/i.java y1/g.java
9	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	g6/c.java q0/o0.java r1/b.java
10	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	s1/i.java
11	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	l1/a1.java
12	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	g6/b.java
13	The file or SharedPreference is World Readable. Any App can read from the file	high	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	q1/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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	s1/d.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00123	Save the response to JSON after connecting to the remote server	network command	s1/a.java s1/b.java s1/g.java s1/i.java
00108	Read the input stream from given URL	network command	com/samsung/android/sdk/internal/healthdata/DeviceUtil.java e7/a.java s1/a.java s1/b.java s1/e.java s1/g.java

RULE ID	BEHAVIOUR	LABEL	FILES
00096	Connect to a URL and set request method	command network	e7/a.java h6/c.java m7/e.java
00089	Connect to a URL and receive input stream from the server	command network	com/bumptech/glide/load/data/j.java com/samsung/android/sdk/internal/healthdata/DeviceUtil.java e7/a.java h6/c.java m7/e.java
00109	Connect to a URL and get the response code	network command	com/bumptech/glide/load/data/j.java com/samsung/android/sdk/internal/healthdata/DeviceUtil.java e7/a.java h6/c.java j3/d.java m7/e.java
00094	Connect to a URL and read data from it	command network	com/samsung/android/sdk/internal/healthdata/DeviceUtil.java e7/a.java
00022	Open a file from given absolute path of the file	file	com/ascensia/contour/MainActivity.java com/ascensia/contour/d.java com/ascensia/contour/editview/EditviewActivity.java com/ascensia/contour/editview/m.java d7/a.java l7/c.java q0/o0.java v0/d.java w0/a.java
00183	Get current camera parameters and change the setting.	camera	com/ascensia/contour/editview/CustomCamera.java com/ascensia/contour/editview/m.java

RULE ID	BEHAVIOUR	LABEL	FILES
00091	Retrieve data from broadcast	collection	com/ascensia/contour/MainActivity.java com/ascensia/contour/NotificationDetailsActivity.java com/ascensia/contour/editview/AddnewActivity.java com/ascensia/contour/editview/CustomCamera.java com/ascensia/contour/editview/EditLocationActivity.java com/ascensia/contour/editview/EditviewActivity.java com/ascensia/contour/reminders/OnAlarmReceiver.java com/ascensia/contour/reportview/ApplicationSelectorReceiver.java
00112	Get the date of the calendar event	collection calendar	com/ascensia/contour/MainActivity.java com/ascensia/contour/d.java com/ascensia/contour/editview/EditviewActivity.java com/ascensia/contour/reminders/OnAlarmReceiver.java l1/b.java q1/a.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/ascensia/contour/InternalWebActivity.java com/ascensia/contour/MainActivity.java com/ascensia/contour/PopupWebview.java com/ascensia/contour/editview/ImageCropActivity.java com/samsung/android/sdk/healthdata/HealthConnectionErrorResult.java n1/e.java q3/i1.java s1/j.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	z1/c.java
00014	Read file into a stream and put it into a JSON object	file	com/ascensia/contour/MainActivity.java com/ascensia/contour/d.java g6/c.java s1/g.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	com/ascensia/contour/MainActivity.java com/ascensia/contour/d.java com/bumptech/glide/load/a.java com/samsung/android/sdk/internal/healthdata/DeviceUtil.java e2/g.java g6/c.java l7/c.java q0/o0.java s0/b.java s1/g.java s1/h.java s1/k.java w1/a.java
00005	Get absolute path of file and put it to JSON object	file	com/ascensia/contour/MainActivity.java com/ascensia/contour/d.java
00016	Get location info of the device and put it to JSON object	location collection	u1/e.java
00023	Start another application from current application	reflection control	com/ascensia/contour/MainActivity.java
00015	Put buffer stream (data) to JSON object	file	com/ascensia/contour/MainActivity.java
00202	Make a phone call	control	com/ascensia/contour/MainActivity.java
00192	Get messages in the SMS inbox	sms	com/ascensia/contour/MainActivity.java
00203	Put a phone number into an intent	control	com/ascensia/contour/MainActivity.java

RULE ID	BEHAVIOUR	LABEL	FILES
00009	Put data in cursor to JSON object	file	com/ascensia/contour/MainActivity.java
00024	Write file after Base64 decoding	reflection file	com/ascensia/contour/MainActivity.java
00004	Get filename and put it to JSON object	file collection	com/ascensia/contour/MainActivity.java
00012	Read data and put it into a buffer stream	file	com/ascensia/contour/MainActivity.java
00175	Get notification manager and cancel notifications	notification	com/ascensia/contour/MainActivity.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/ascensia/contour/MainActivity.java q3/i1.java
00191	Get messages in the SMS inbox	sms	com/ascensia/contour/MainActivity.java
00036	Get resource file from res/raw directory	reflection	com/ascensia/contour/MainActivity.java
00078	Get the network operator name	collection telephony	j7/b.java
00132	Query The ISO country code	telephony collection	j7/b.java
00072	Write HTTP input stream into a file	command network file	s1/e.java s1/g.java

RULE ID	BEHAVIOUR	LABEL	FILES
00030	Connect to the remote server through the given URL	network	com/bumptech/glide/load/data/j.java com/samsung/android/sdk/internal/healthdata/DeviceUtil.java m7/e.java s1/i.java
00163	Create new Socket and connecting to it	socket	s1/b.java s1/c.java s1/h.java s1/i.java s1/k.java
00162	Create InetSocketAddress object and connecting to it	socket	s1/i.java
00002	Open the camera and take picture	camera	com/ascensia/contour/editview/CustomCamera.java
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	com/ascensia/contour/editview/CustomCamera.java
00121	Create a directory	file command	com/ascensia/contour/editview/EditviewActivity.java
00125	Check if the given file path exist	file	com/ascensia/contour/editview/EditviewActivity.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/342326655623/namespaces/firebase:fetch?key=AIzaSyDo82wjSZ4GnLxC4VV3e_oyXwoIwE8lt3o. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	12/25	android.permission.WRITE_EXTERNAL_STORAGE, android.permission.CAMERA, android.permission.WAKE_LOCK, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.READ_PHONE_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.INTERNET, android.permission.READ_CONTACTS, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION, android.permission.GET_ACCOUNTS
Other Common Permissions	7/44	android.permission.BLUETOOTH, android.permission.BLUETOOTH_ADMIN, android.permission.CALL_PHONE, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, com.google.android.gms.permission.AD_ID, android.permission.FOREGROUND_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

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
contourcloudasia.ascensia.com	ok	**IP:** 168.63.254.148 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** Google Map
contourcloudrussia.ascensia.com	ok	**IP:** 91.227.152.178 **Country:** Russian Federation **Region:** Moskovskaya oblast' **City:** Dolgoprudnyy **Latitude:** 55.904110 **Longitude:** 37.560638 **View:** Google Map
contact.ascensia.com	ok	**IP:** 165.160.13.20 **Country:** United States of America **Region:** Delaware **City:** Wilmington **Latitude:** 39.735779 **Longitude:** -75.665703 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
plus.google.com	ok	**IP:** 64.233.185.138 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
issuetracker.google.com	ok	**IP:** 64.233.177.102 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
play.google.com	ok	**IP:** 172.253.124.113 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.w3.org	ok	**IP:** 104.18.23.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
contourcloudeu.ascensia.com	ok	**IP:** 20.199.123.212 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
developer.android.com	ok	**IP:** 64.233.176.102 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
contourone.com	ok	**IP:** 217.114.94.2 **Country:** Sweden **Region:** Stockholms lan **City:** Stockholm **Latitude:** 59.332581 **Longitude:** 18.064899 **View:** Google Map
docs.google.com	ok	**IP:** 173.194.219.138 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
pagead2.googlesyndication.com	ok	**IP:** 172.253.124.156 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
contourstagingcloud.ascensia.com	ok	**IP:** 20.185.151.8 **Country:** United States of America **Region:** Virginia **City:** Washington **Latitude:** 38.713451 **Longitude:** -78.159439 **View:** Google Map
contourcloudazuredev.ascensia.com	ok	**IP:** 20.185.151.8 **Country:** United States of America **Region:** Virginia **City:** Washington **Latitude:** 38.713451 **Longitude:** -78.159439 **View:** Google Map
ec.europa.eu	ok	**IP:** 147.67.34.30 **Country:** Luxembourg **Region:** Luxembourg **City:** Luxembourg **Latitude:** 49.611671 **Longitude:** 6.130000 **View:** Google Map
onyxtestcloud.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
hub.samsungapps.com	ok	**IP:** 54.77.39.19 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map
contourtestcloud.com	ok	No Geolocation information available.
in.appcenter.ms	ok	**IP:** 68.220.193.245 **Country:** United States of America **Region:** Georgia **City:** Atlanta **Latitude:** 33.818501 **Longitude:** -84.361015 **View:** Google Map
schemas.microsoft.com	ok	**IP:** 13.107.253.71 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
contourapplb.contourcloud.com	ok	**IP:** 69.64.147.244 **Country:** United States of America **Region:** Washington **City:** Bellevue **Latitude:** 47.615639 **Longitude:** -122.210876 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
contourcloudus.ascensia.com	ok	**IP:** 20.124.191.46 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map

✉ EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	n3/t.java
privacy@ascensia.com info@ascensia.de parent.email@email.com	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Microsoft Visual Studio App Center Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/243

TRACKER	CATEGORIES	URL
Microsoft Visual Studio App Center Crashes	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/238

HARDCODED SECRETS

POSSIBLE SECRETS
"comm_onyxpassword" : "password"
"comm_password" : "Password"
"comm_turkey" : "Turkey"
"firebase_preference_file_key" : "com.microsoft.windowsazure.messaging.notificationhubs.FirebasePreferences"
"google_api_key" : "AIzaSyDo82wjSZ4GnLxC4VV3e_oyXwoIwE8lt3o"
"google_crash_reporting_api_key" : "AIzaSyDo82wjSZ4GnLxC4VV3e_oyXwoIwE8lt3o"
"hcpkey" : "KEY"
"installation_enrichment_file_key" : "com.microsoft.windowsazure.messaging.notificationhubs.InstallationSharedPreferences"
"optumrx_header_registereduser" : "OptumRx"

POSSIBLE SECRETS
308204a830820390a003020102020900936eacbe07f201df300d06092a864886f70d0101050500308194310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d301e170d3038303232393031333334365a170d3335303731373031333334365a308194310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d30820120300d06092a864886f70d01010105000382010d00308201080282010100d6931904dec60b24b1edc762e0d9d8253e3ecd6ceb1de2ff068ca8e8bca8cd6bd3786ea70aa76ce60ebb0f993559ffd93e77a943e7e83d4b64b8e4fea2d3e656f1e267a81bbfb230b578c20443be4c7218b846f5211586f038a14e89c2be387f8ebecf8fcac3da1ee330c9ea93d0a7c3dc4af350220d50080732e0809717ee6a053359e6a694ec2cb3f284a0a466c87a94d83b31093a67372e2f6412c06e6d42f15818dffe0381cc0cd444da6cddc3b82458194801b32564134fbfde98c9287748dbf5676a540d8154c8bbca07b9e247553311c46b9af76fdeeccc8e69e7c8a2d08e782620943f99727d3c04fe72991d99df9bae38a0b2177fa31d5b6afee91f020103a381fc3081f9301d0603551d0e041604148 5900563d272c46ae118605a47419ac09ca8c113081c90603551d230481c13081be8014485900563d272c46ae118605a47419ac09ca8c11a1819aa48197308194310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d820900936eacbe07f201df300c0603551d13040530030101ff300d06092a864886f70d010105050003820101007aaf968ceb50c441055118d0daabaf015b8a765a27a715a2c2b44f221415ffdace03095abfa42df70708726c2069e5c36eddae0400be29452c084bc27eb6a17eac9dbe182c204eb15311f455d824b656dbe4dc2240912d7586fe88951d01a8feb5ae5a4260535df83431052422468c36e22c2a5ef994d61dd7306ae4c9f6951ba3c12f1d1914ddc61f1a62da2df827f603fea5603b2c540dbd7c019c36bab29a4271c117df523cdbc5f3817a49e0efa60cbd7f74177e7a4f193d43f4220772666e4c4d83e1bd5a86087cf34f2dec21e245ca6c2bb016e683638050d2c430eea7c26a1c49d3760a58ab7f1a82cc938b4831384324bd0401fa12163a50570e684d
d9027d96179d9d391d05ef97d7177ba316c18fba
SharedAccessKey=lw2shvGWWr496vvrJrf2lR4YUTQBZ6lA9C2of27y2lg=
0630f4ff56a7003ee908e03e976808e44228b15a
564442af86a06640d1ae20c1c09b24aa581460f4
74e88930ff8d976037c205609699b7ace7872190
771f8179194bbe56c9455f32c984f8f54e535696
ff80efd2c5b48306482d04610cb0f818e552f906

POSSIBLE SECRETS
ae2044fb577e65ee8bb576ca48a2f06e
7b19dff679e73e8e6e404dab21beb2a9aa47a6ac
620e341d488a37479d964b3dadbd0d88206f7f63
1352b6033d7e72f8d36939d07b97aef9e07ed493
df3c81cb26341ea21b57c0db87fa6dc80dac44da
308204a830820390a003020102020900b3998086d056cffa300d06092a864886f70d0101040500308194310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d301e170d3038303431353232343035305a170d3335303930313232343035305a308194310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d30820120300d06092a864886f70d01010105000382010d00308201080282010100c780592ac0d5d381cdeaa65ecc8a6006e36480c6d7207b12011be50863aabe2b55d009adf7146d6f2202280c7cd4d7bdb26243b8a806c26b34b137523a49268224904dc01493e7c0acf1a05c874f69b037b60309d9074d24280e16bad2a8734361951eaf72a482d09b204b1875e12ac98c1aa773d6800b9eafde56d58bed8e8da16f9a360099c37a834a6dfedb7b6b44a049e07a269fccf2c5496f2cf36d64df90a3b8d8f34a3baab4cf53371ab27719b3ba58754ad0c53fc14e1db45d51e234fbbe93c9ba4edf9ce54261350ec535607bf69a2ff4aa07db5f7ea200d09a6c1b49e21402f89ed1190893aab5a9180f152e82f85a45753cf5fc19071c5eec827020103a381fc3081f9301d0603551d0e041604144fe4a0b3dd9cba29f71d7287c4e7c38f2086c2993081c90603551d230481c13081be80144fe4a0b3dd9cba29f71d7287c4e7c38f2086c299a1819aa48197308194310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d820900b3998086d056cffa300c0603551d13040530030101ff300d06092a864886f70d01010405000382010100572551b8d93a1f73de0f6d469f86dad6701400293c88a0cd7cd778b73dafcc197fab76e6212e56c1c761cfc42fd733de52c50ae08814cefc0a3b5a1a4346054d829f1d82b42b2048bf88b5d14929ef85f60edd12d72d55657e22e3e85d04c831d613d19938bb8982247fa321256ba12d1d6a8f92ea1db1c373317ba0c037f0d1aff645aef224979fba6e7a14bc025c71b98138cef3ddfc059617cf24845cf7b40d6382f7275ed738495ab6e5931b9421765c491b72fb68e080dbdb58c2029d347c8b328ce43ef6a8b15533edfbe989bd6a48dd4b202eda94c6ab8dd5b8399203daae2ed446232e4fe9bd961394c6300e5138e3cfd285e6e4e483538cb8b1b357
3d6c7814dcdb0480e597bc7e030b5373ce13d59b
5181942b9ebc31ce68dacb56c16fd79f

POSSIBLE SECRETS
9ecd11ecd6411a620f5b72f512e8925b8a7e3c6f
371e1118060bd749039aa377b76dbfcf2cd594cc
65c3752200d4d41927bc6864d7774d5aa4185e3a
308204d4308203bca003020102020900d20995a79c0daad6300d06092a864886f70d01010505003081a2310b3009060355040613024b52311430120603550408130b536f757468204b6f726561311330110603550407130a5375776f6e2043697479311c301a060355040a131353616d73756e6720436f72706f726174696f6e310c300a060355040b1303444d43311530130603550403130c53616d73756e6720436572743125302306092a864886f70d0109011616616e64726f69642e6f734073616d73756e672e636f6d301e170d3131303632323132323531325a170d3338313130373132323531325a3081a2310b3009060355040613024b52311430120603550408130b536f757468204b6f726561311330110603550407130a5375776f6e2043697479311c301a060355040a131353616d73756e6720436f72706f726174696f6e310c300a060355040b1303444d43311530130603550403130c53616d73756e6720436572743125302306092a864886f70d0109011616616e64726f69642e6f734073616d73756e672e636f6d30820120300d06092a864886f70d01010105000382010d00308201080282010100c986384a3e1f2fb206670e78ef232215c0d26f45a22728db99a44da11c35ac33a71fe071c4a2d6825a9b4c88b333ed96f3c5e6c666d60f3ee94c490885abcf8dc660f707aabc77ead3e2d0d8aee8108c15cd260f2e85042c28d2f292daa3c6da0c7bf2391db7841aade8fdf0c9d0defcf77124e6d2de0a9e0d2da746c3670e4ffcdc85b701bb4744861b96ff7311da3603c5a10336e55ffa34b4353eedc85f51015e1518c67e309e39f87639ff178107f109cd18411a6077f26964b6e63f8a70b9619db04306a323c1a1d23af867e19f14f570ffe573d0e3a0c2b30632aaec3173380994be1e341e3a90bd2e4b615481f46db39ea83816448ec35feb1735c1f3020103a382010b30820107301d0603551d0e04160414932c3af70b627a0c7610b5a0e7427d6cfaea3f1e3081d70603551d230481cf3081cc8014932c3af70b627a0c7610b5a0e7427d6cfaea3f1ea181a8a481a53081a2310b3009060355040613024b52311430120603550408130b536f757468204b6f726561311330110603550407130a5375776f6e2043697479311c301a060355040a131353616d73756e6720436f72706f726174696f6e310c300a060355040b1303444d43311530130603550403130c53616d73756e6720436572743125302306092a864886f70d0109011616616e64726f69642e6f734073616d73756e672e636f6d820900d20995a79c0daad6300c0603551d13040530030101ff300d06092a864886f70d01010505000382010100329601fe40e036a4a86cc5d49dd8c1b5415998e72637538b0d430369ac51530f63aace8c019a1a66616a2f1bb2c5fabd6f313261f380e3471623f053d9e3c53f5fd6d1965d7b000e4dc244c1b27e2fe9a323ff077f52c4675e86247aa801187137e30c9bbf01c567a4299db4bf0b25b7d7107a7b81ee102f72ff47950164e26752e114c42f8b9d2a42e7308897ec640ea1924ed13abbe9d120912b62f4926493a86db94c0b46f44c6161d58c2f648164890c512dfb28d42c855bf470dbee2dab6960cad04e81f71525ded46cdd0f359f99c460db9f007d96ce83b4b218ac2d82c48f12608d469733f05a3375594669ccbf8a495544d6c5701e9369c08c810158
2f9734ce154afe2b02776f1e6e019382586c7cb9

POSSIBLE SECRETS
308204d4308203bca003020102020900e5eff0a8f66d92b3300d06092a864886f70d01010505003081a2310b30090603550406130244b5231143012060355040813bb536f757468204b6f72656131133011060355040713a5375776f6e2043697479311c301a060355040a131353616d73756e6720436f72706f726174696f6e310c300a060355040b1303444d433115301306035504030c53616d73756e6720436572743125302306092a864886f70d0109011616616e64726f69642e6f734073616d73756e672e636f6d301e170d3131303632323132323531335a170d3338313130373132323531335a3081a2310b30090603550406130244b5231143012060355040813bb536f757468204b6f72656131133011060355040713a5375776f6e2043697479311c301a060355040a131353616d73756e6720436f72706f726174696f6e310c300a060355040b1303444d433115301306035504030c53616d73756e6720436572743125302306092a864886f70d0109011616616e64726f69642e6f734073616d73756e672e636f6d30820120300d06092a864886f70d01010105000382010d00308201080282010100e9f1edb42423201dce62e68f2159ed8ea766b43a43d348754841b72e9678ce6b03d06d31532d88f2ef2d5ba39a028de0857983cd321f5b7786c2d3699df4c0b40c8d856f147c5dc54b9d1d671d1a51b5c5364da36fc5b0fe825afb513ec7a2db862c48a6046c43c3b71a1e275155f6c30aed2a68326ac327f60160d427cf55b617230907a84edbff21cc256c628a16f15d55d49138cdf2606504e1591196ed0bdc25b7cc4f67b33fb29ec4dbb13dbe6f3467a0871a49e620067755e6f095c3bd84f8b7d1e66a8c6d1e5150f7fa9d95475dc7061a321aaf9c686b09be23ccc59b35011c6823ffd5874d8fa2a1e5d276ee5aa381187e26112c7d5562703b36210b020103a382010b30820107301d0603551d0e041604145b115b23db35655f9f77f78756961006eebe3a9e3081d70603551d230481cf3081cc80145b115b23db35655f9f77f78756961006eebe3a9ea181a8a481a53081a2310b30090603550406130244b5231143012060355040813bb536f757468204b6f72656131133011060355040713a5375776f6e2043697479311c301a060355040a131353616d73756e6720436f72706f726174696f6e310c300a060355040b1303444d433115301306035504030c53616d73756e6720436572743125302306092a864886f70d0109011616616e64726f69642e6f734073616d73756e672e636f6d820900e5eff0a8f66d92b3300c0603551d13040530030101ff300d06092a864886f70d0101050500038201010039c91877eb09c2c84445443673c77a1219c5c02e6552fa2fbad0d736bc5ab6ebaf0375e520fe9799403ecb71659b23afda1475a34ef4b2e1ffcba8d7ff385c21cb6482540bce3837e6234fd4f7dd576d7fcfe9cfa925509f772c494e1569fe44e6fcd4122e483c2caa2c639566dbcfe85ed7818d5431e73154ad453289fb56b607643919cf534fbeefbdc2009c7fcb5f9b1fa97490462363fa4bedc5e0b9d157e448e6d0e7cfa31f1a2faa9378d03c8d1163d3803bc69bf24ec77ce7d559abcaf8d345494abf0e3276f0ebd2aa08e4f4f6f5aaea4bc523d8cc8e2c9200ba551dd3d4e15d5921303ca9333f42f992ddb70c2958e776c12d7e3b7bd74222eb5c7a
308201e53082014ea00302010202044f54468b300d06092a864886f70d01010505003037310b30090603550406130255533110300e060355040a1307416e64726f6964311630140603550403130d416e64726f6964204465627567301e170d3132303330353034353232375a170d3432303232363034353232375a3037310b30090603550406130255533110300e060355040a1307416e64726f6964311630140603550403130d416e64726f696420446562756730819f300d06092a864886f70d010101050003818d0030818902818100 8a53be36d02befe1d152724281630bd1c42eff0edf5fdca8eb944f536ab3f54dca9b22cfb421b37706a4ad259101815723202b359250cf6c59905032798273462bfa3f9f1881f7475ee5b25849edefac81085815f42383a44cb2be1bfd5c1f049ef42f5818f35fe0b1131c769cee347d558395a5fa87c3d425b2b9c819cf91870203010001300d06092a864886f70d0101050500038181000512992268a01e0941481931f3f9b6647fbe25ee0bc9648f35d56c55f8cfa6c935fb3d435125fd60ef566769ac7e64fe2823409461ca7a04570c43baaab3fb877bf3a6a8dd9ef7e69944f65b0e5e36f2ac2bf085fdeda063898855ea2ce84c60655d824844fe1659a77c12604c3fb84d41df6f1a7705a1b9962ac2fdc9933122
31b1f5436d02a0fd9957d08d0abeb5c4cab31d79
c4d6e977537e83d7dcc003313af6543755e2126a

PLAYSTORE INFORMATION

Title: CONTOUR DIABETES app (US)

Score: 3.4310954 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.ascensia.contour.us

Developer Details: Ascensia Diabetes Care, Ascensia+Diabetes+Care, None, http://diabetes.ascensia.com, websiteinfo@ascensia.com,

Release Date: Dec 28, 2016 **Privacy Policy:** Privacy link

Description:

The easy-to-use CONTOUR™DIABETES app is designed for adults of all ages with diabetes.(1) Since 2016, there have been over 1.2 million downloads.(2) Start your download and enjoy your journey. People using the system say they:(1,3) • better understood their diabetes • significantly decreased HbA1c values • didn't find it to be a hassle that compromised their quality of life The CONTOUR™DIABETES app syncs with a CONTOUR™ connected meter for seamless blood glucose monitoring. This easy-to-use app can give you a better understanding of how your daily activities affect your blood glucose results to help you manage your diabetes. In addition to using the CONTOUR™DIABETES app, always consult with your Health Care Professional before making any changes to your diet, exercise or treatment regimen. The CONTOUR™DIABETES app presents your blood glucose results in a simple and easy-to-review way that's personalized to you. Download the CONTOUR™DIABETES app today and start receiving meaningful information on your progress, with some of the latest features… • My Patterns – can notify you of trends in your blood glucose readings, by presenting you with potential causes and guidance on how you may improve • Test Reminder Plans – let you optimize your testing regime to give you results that are more insightful • Record – allows you to record events such as diet, activities and medication, and also add photos, notes or voice memos to help put your results in context • View – if you use insulin and/or log your carbs, you can now see your insulin doses, carb intakes and blood glucose results in one simple view • Share – give your healthcare professional greater insight with the easy-to-read diary report – send this report in advance or take it with you on the day of your appointment • Apple Health™ - is now integrated with the CONTOUR™DIABETES app Learn more about the CONTOUR™DIABETES app and CONTOUR™ connected meters at: www.diabetes.ascensia.com compatibility.contourone.com Note: Screenshots are for illustration purposes. Availability of blood glucose meter model based on country of purchase. Units of measurement in the app will match that of your synced meter. For more information, please refer to the user guide for your CONTOUR™ connected meter. © 2021 Ascensia Diabetes Care Holdings AG. All rights reserved. Manufacturer Ascensia Diabetes Care Holdings AG 5 Wood Hollow Rd. Parsippany, NJ 07054 www.contourone.com Ascensia, the Ascensia Diabetes Care logo and Contour are trademarks and/or registered trademarks of Ascensia Diabetes Care Holdings AG. 1. Fisher W et al. User Experience with a New Smartphone Application for Blood Glucose Monitoring (BGM) in an Information-Motivation-Behavioral Skills (IMB) Model Study. Poster presented at the 12th International Conference on Advanced Technologies & Treatments For Diabetes (ATTD); February 20-23, 2019; Berlin, Germany. 2. Data on file. Ascensia Diabetes Care. DCAM-147-5682. 3. Fernandez-Garcia D et al. The ICONE Study: A multicenter evaluation of the impact of CONTOUR™NEXT ONE and CONTOUR™DIABETES app on Self-Management and Adherence in Insulin-Treated Patients with Diabetes. ePoster presented at European Endocrinology Society Congress (ECE), 5-9 September 2020.

SCAN LOGS

Timestamp	Event	Error
2025-08-29 19:56:39	Generating Hashes	OK
2025-08-29 19:56:39	Extracting APK	OK
2025-08-29 19:56:39	Unzipping	OK
2025-08-29 19:56:39	Parsing APK with androguard	OK
2025-08-29 19:56:40	Extracting APK features using aapt/aapt2	OK
2025-08-29 19:56:40	Getting Hardcoded Certificates/Keystores	OK
2025-08-29 19:56:42	Parsing AndroidManifest.xml	OK
2025-08-29 19:56:42	Extracting Manifest Data	OK
2025-08-29 19:56:42	Manifest Analysis Started	OK
2025-08-29 19:56:42	Reading Network Security config from network_security_config.xml	OK

2025-08-29 19:56:42	Parsing Network Security config	OK
2025-08-29 19:56:42	Performing Static Analysis on: Contour (com.ascensia.contour.us)	OK
2025-08-29 19:56:43	Fetching Details from Play Store: com.ascensia.contour.us	OK
2025-08-29 19:56:43	Checking for Malware Permissions	OK
2025-08-29 19:56:43	Fetching icon path	OK
2025-08-29 19:56:43	Library Binary Analysis Started	OK
2025-08-29 19:56:44	Reading Code Signing Certificate	OK
2025-08-29 19:56:44	Running APKiD 2.1.5	OK
2025-08-29 19:56:47	Detecting Trackers	OK
2025-08-29 19:56:48	Decompiling APK to Java with JADX	OK
2025-08-29 19:56:57	Converting DEX to Smali	OK

2025-08-29 19:56:57	Code Analysis Started on - java_source	OK
2025-08-29 19:56:58	Android SBOM Analysis Completed	OK
2025-08-29 19:57:02	Android SAST Completed	OK
2025-08-29 19:57:02	Android API Analysis Started	OK
2025-08-29 19:57:07	Android API Analysis Completed	OK
2025-08-29 19:57:07	Android Permission Mapping Started	OK
2025-08-29 19:57:13	Android Permission Mapping Completed	OK
2025-08-29 19:57:13	Android Behaviour Analysis Started	OK
2025-08-29 19:57:21	Android Behaviour Analysis Completed	OK
2025-08-29 19:57:21	Extracting Emails and URLs from Source Code	OK

2025-08-29 19:57:22	Email and URL Extraction Completed	OK
2025-08-29 19:57:22	Extracting String data from APK	OK
2025-08-29 19:57:22	Extracting String data from Code	OK
2025-08-29 19:57:22	Extracting String values and entropies from Code	OK
2025-08-29 19:57:24	Performing Malware check on extracted domains	OK
2025-08-29 19:57:25	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.