MOBSF

ANDROID STATIC ANALYSIS REPORT

KT Mobile (9.3)

File Name:	com.kanrad.kantimemobile_1245.apk
Package Name:	com.kanrad.kantimemobile
Scan Date:	Aug. 30, 2025, 10:33 p.m.
App Security Score:	45/100 (MEDIUM RISK)
Grade:	
Trackers Detection:	2/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	11	3	0	1

FILE INFORMATION

File Name: com.kanrad.kantimemobile_1245.apk
Size: 33.11MB
MD5: 17edc7b69d20f9ba892d79919f916681
SHA1: 1528dfee442ea20ecd537e91093464ac3952280b
SHA256: 4fef5971f8585046ae0acb205bb09073be7f1bebba1e008a7a57a591a5803da2

APP INFORMATION

App Name: KT Mobile
Package Name: com.kanrad.kantimemobile
Main Activity: crc64f505b029e5a01cf8.SplashActivity
Target SDK: 34
Min SDK: 21
Max SDK:
Android Version Name: 9.3

Android Version Code: 1245

APP COMPONENTS

Activities: 60
Services: 7
Receivers: 8
Providers: 3
Exported Activities: 0
Exported Services: 1
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=91, ST=Karnataka, L=Bangalore, O=Kanrad Technologies Inc., OU=KMobile, CN=Sundar Kannan
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2016-02-05 08:05:11+00:00
Valid To: 2116-01-12 08:05:11+00:00
Issuer: C=91, ST=Karnataka, L=Bangalore, O=Kanrad Technologies Inc., OU=KMobile, CN=Sundar Kannan
Serial Number: 0x56b457b7
Hash Algorithm: sha1
md5: 06b4aaf4dc6985e8b7f3d7b61a38703e
sha1: a7f82ceeeed801b8c165aea1d31080fc768c09a4
sha256: 97a0d3a4d46f9f2ab3563d9663d4f7cf8916c328c3a16b43738ceab3c5e3db36
sha512: 58c0f23593c18561a0f47eb63a0598b9f9b8db48f929a581de415819e428027939b51a0489535cb4484cc9dbadfbe15b50a3efd6609395f18f23a62a4f246f4b
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 29c626b2abcf0a738d47239756c0c047b6ed0f98e2cfd7c497e3312c7a868550
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_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.kanrad.kantimemobile.permission.C2D_MESSAGE	unknown	Unknown permission	Unknown permission from android reference
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.ACCESS_MEDIA_LOCATION	dangerous	access any geographic locations	Allows an application to access any geographic locations persisted in the user's shared collection.
android.permission.MANAGE_MEDIA	signature	allows modification and deletion of media files without user confirmation.	Allows an application to modify and delete media files on this device or any connected storage device without user confirmation. Applications must already be granted the READ_EXTERNAL_STORAGE or MANAGE_EXTERNAL_STORAGE } permissions for this permission to take effect.
android.permission.MEDIA_CONTENT_CONTROL	normal	allows control over media content playback.	Allows an application to know what content is playing and control its playback.
android.permission.READ_MEDIA_AUDIO	dangerous	allows reading audio files from external storage.	Allows an application to read audio files from external storage.
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.READ_MEDIA_VIDEO	dangerous	allows reading video files from external storage.	Allows an application to read video files from external storage.

PERMISSION	STATUS	INFO	DESCRIPTION
com.sec.android.provider.badge.permission.READ	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.sec.android.provider.badge.permission.WRITE	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.htc.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.htc.launcher.permission.UPDATE_SHORTCUT	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.sonyericsson.home.permission.BROADCAST_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.anddoes.launcher.permission.UPDATE_COUNT	normal	show notification count on app	Show notification count or badge on application launch icon for apex.
com.majeur.launcher.permission.UPDATE_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for solid.
com.huawei.android.launcher.permission.CHANGE_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.huawei.android.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.huawei.android.launcher.permission.WRITE_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_APP_BADGE	normal	show app notification	Allows an application to show app icon badges.
com.oppo.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for oppo phones.
com.oppo.launcher.permission.WRITE_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for oppo phones.
me.everything.badger.permission.BADGE_COUNT_READ	unknown	Unknown permission	Unknown permission from android reference
me.everything.badger.permission.BADGE_COUNT_WRITE	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check Build.MANUFACTURER check Build.HARDWARE check network operator name check possible VM check FINDINGS: Compiler — DETAILS: r8 without marker (suspicious)

FILE	DETAILS

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 2 | 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.

TITLE	SEVERITY	DESCRIPTION
Certificate algorithm might be vulnerable to hash collision	warning	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues. The manifest file indicates SHA256withRSA is in use.

MANIFEST ANALYSIS

HIGH: 1 | WARNING: 4 | 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	Broadcast Receiver (com.google.android.gms.gcm.GcmReceiver) 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.
3	Service (crc647328f41b9c5562ef.ExitListenerService) 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 (crc647328f41b9c5562ef.GenericBroadcastReceiver) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
5	Broadcast Receiver (crc647328f41b9c5562ef.HomeButtonReceiver) 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.

</> CODE ANALYSIS

HIGH: 0 | WARNING: 3 | INFO: 3 | SECURE: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/microsoft/appcenter/AbstractAppCenterService.java com/microsoft/appcenter/AppCenter.java com/microsoft/appcenter/Constants.java com/microsoft/appcenter/CustomProperties.java com/microsoft/appcenter/SessionContext.java com/microsoft/appcenter/analytics/Analytics.java com/microsoft/appcenter/analytics/channel/SessionTracker.java com/microsoft/appcenter/analytics/ingestion/models/EventLog.java com/microsoft/appcenter/channel/DefaultChannel.java com/microsoft/appcenter/crashes/Crashes.j

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	ava com/microsoft/appcenter/crashes/WrapperSdkExceptionManager.java com/microsoft/appcenter/crashes/ingestion/models/AbstractErrorLog.java com/microsoft/appcenter/crashes/ingestion/models/ErrorAttachmentLog.java com/microsoft/appcenter/crashes/ingestion/models/HandledErrorLog.java com/microsoft/appcenter/crashes/ingestion/models/ManagedErrorLog.java com/microsoft/appcenter/crashes/utils/ErrorLogHelper.java com/microsoft/appcenter/http/DefaultHttpClient.java com/microsoft/appcenter/http/HttpClientNetworkStateHandler.java com/microsoft/appcenter/http/HttpClientRetryer.java com/microsoft/appcenter/ingestion/IngestionHttp.java com/microsoft/appcenter/ingestion/models/AbstractLog.java com/microsoft/appcenter/ingestion/models/json/DefaultLogSerializer.java com/microsoft/appcenter/persistence/DatabasePersistence.java com/microsoft/appcenter/utils/AppCenterLog.java com/microsoft/appcenter/utils/AsyncTaskUtils.java com/microsoft/appcenter/utils/DeviceInfoHelper.java com/microsoft/appcenter/utils/IdHelper.java com/microsoft/appcenter/utils/NetworkStateHelper.java com/microsoft/appcenter/utils/UUIDUtils.java com/microsoft/appcenter/utils/crypto/CryptoUtils.java com/microsoft/appcenter/utils/storage/Data

NO	ISSUE	SEVERITY	STANDARDS	FILES
				baseManager.java com/microsoft/appcenter/utils/storage/StorageHelper.java me/leolin/shortcutbadger/ShortcutBadger.java mono/android/incrementaldeployment/IncrementalClassLoader.java
2	This App uses SQL Cipher. Ensure that secrets are not hardcoded in code.	info	OWASP MASVS: MSTG-CRYPTO-1	com/microsoft/appcenter/utils/storage/DatabaseManager.java
3	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/microsoft/appcenter/utils/storage/DatabaseManager.java
4	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/microsoft/appcenter/SessionContext.java com/microsoft/appcenter/http/DefaultHttpClient.java com/microsoft/appcenter/ingestion/IngestionHttp.java com/microsoft/appcenter/ingestion/models/WrapperSdk.java com/microsoft/appcenter/utils/storage/DatabaseManager.java
5	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/microsoft/appcenter/http/HttpClientRetryer.java com/microsoft/appcenter/utils/UUIDUtils.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
6	This app listens to Clipboard changes. Some malware also listen to Clipboard changes.	info	OWASP MASVS: MSTG-PLATFORM-4	crc64a0e0a82d0db9a07d/ClipboardChangeListener.java mono/android/content/ClipboardManager_OnPrimaryClipChangedListenerImplementor.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	me/leolin/shortcutbadger/impl/OPPOHomeBader.java me/leolin/shortcutbadger/impl/SonyHomeBadger.java
00036	Get resource file from res/raw directory	reflection	me/leolin/shortcutbadger/impl/EverythingMeHomeBadger.java me/leolin/shortcutbadger/impl/HuaweiHomeBadger.java me/leolin/shortcutbadger/impl/NovaHomeBadger.java me/leolin/shortcutbadger/impl/OPPOHomeBader.java me/leolin/shortcutbadger/impl/SamsungHomeBadger.java me/leolin/shortcutbadger/impl/SonyHomeBadger.java
00022	Open a file from given absolute path of the file	file	com/microsoft/appcenter/crashes/Crashes.java com/microsoft/appcenter/crashes/utils/ErrorLogHelper.java com/microsoft/appcenter/utils/storage/StorageHelper.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	com/microsoft/appcenter/utils/storage/StorageHelper.java
00078	Get the network operator name	collection telephony	com/microsoft/appcenter/utils/DeviceInfoHelper.java
00132	Query The ISO country code	telephony collection	com/microsoft/appcenter/utils/DeviceInfoHelper.java
00189	Get the content of a SMS message	sms	me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00188	Get the address of a SMS message	sms	me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00191	Get messages in the SMS inbox	sms	me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00200	Query data from the contact list	collection contact	me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00187	Query a URI and check the result	collection sms calllog calendar	me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00201	Query data from the call log	collection calllog	me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00096	Connect to a URL and set request method	command network	com/microsoft/appcenter/http/DefaultHttpClient.java
00089	Connect to a URL and receive input stream from the server	command network	com/microsoft/appcenter/http/DefaultHttpClient.java

RULE ID	BEHAVIOUR	LABEL	FILES
00109	Connect to a URL and get the response code	network command	com/microsoft/appcenter/http/DefaultHttpClient.java
00094	Connect to a URL and read data from it	command network	com/microsoft/appcenter/http/DefaultHttpClient.java
00108	Read the input stream from given URL	network command	com/microsoft/appcenter/http/DefaultHttpClient.java

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	9/25	android.permission.INTERNET, android.permission.ACCESS_WIFI_STATE, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION, android.permission.WAKE_LOCK, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.RECORD_AUDIO
Other Common Permissions	1/44	com.google.android.c2dm.permission.RECEIVE

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
in.appcenter.ms	ok	**IP:** 4.152.45.207 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map

TRACKERS

TRACKER	CATEGORIES	URL
Microsoft Visual Studio App Center Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/243
Microsoft Visual Studio App Center Crashes	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/238

HARDCODED SECRETS

POSSIBLE SECRETS
"Password" : "Password"
"Vitals_Key" : "Vitals_key"
"ConfiguringUser" : "□□□□□□□....."
"DELETEUSER" : "□□□□"
"Password" : "□□"
"PatientToleratedSessionWell" : "□□□□□□□□"
"RegisterUser" : "□□□□"
"Vitals_Key" : "□□□□_□"
"Password" : "Contraseña"

PLAYSTORE INFORMATION

Title: KanTime Mobile

Score: 3.43 **Installs:** 10,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.kanrad.kantimemobile

Developer Details: Kanrad Technologies Inc., 5333275872195002135, None, http://www.kantime.com, kantimemobile@kanrad.com,

Release Date: Mar 29, 2016 **Privacy Policy:** Privacy link

Description:

KanTime Mobile: Empowering Clinicians On-the-Go Streamline Your Patient Care with KanTime Mobile – the ultimate app designed for healthcare professionals. With KanTime Mobile, managing patient schedules and visits is effortless, even offline. Our intuitive platform is crafted for caregivers, enabling seamless Check-ins and Check-

outs directly from your mobile device. Features That Enhance Your Efficiency • Offline Mode: Stay Connected, Even Offline - Perform all tasks without an internet connection and sync effortlessly with KanTime Live once you're back online. • Timesheet Management: Document Check-in/Check-out, travel time, and miles. Capture client signatures with ease. o EVV Check-in/Check-out: Validate check-in/out time-stamped verifications with precision, meeting all state and federal EVV requirements • Task Documentation: Record daily aide tasks quickly and accurately. • Geo-Fencing: Automatic location validation for accurate Check-ins. • Data Sync: Consolidating all your data with a single tap ensures all your information is updated and secure. • HIPAA-Compliant: Adhere to stringent healthcare regulations for patient data confidentiality. • Data Integrity: We employ rigorous protocols to maintain the accuracy and completeness of your data throughout its lifecycle. KanTime Mobile is more than just an app; it's your partner in delivering exceptional patient care. Download now and take the first step towards a more organized and efficient caregiving experience.

SCAN LOGS

Timestamp	Event	Error
2025-08-30 22:33:24	Generating Hashes	OK
2025-08-30 22:33:24	Extracting APK	OK
2025-08-30 22:33:24	Unzipping	OK
2025-08-30 22:33:28	Parsing APK with androguard	OK
2025-08-30 22:33:28	Extracting APK features using aapt/aapt2	OK
2025-08-30 22:33:29	Getting Hardcoded Certificates/Keystores	OK

2025-08-30 22:33:31	Parsing AndroidManifest.xml	OK
2025-08-30 22:33:31	Extracting Manifest Data	OK
2025-08-30 22:33:31	Manifest Analysis Started	OK
2025-08-30 22:33:31	Performing Static Analysis on: KT Mobile (com.kanrad.kantimemobile)	OK
2025-08-30 22:33:32	Fetching Details from Play Store: com.kanrad.kantimemobile	OK
2025-08-30 22:33:32	Checking for Malware Permissions	OK
2025-08-30 22:33:32	Fetching icon path	OK
2025-08-30 22:33:32	Library Binary Analysis Started	OK
2025-08-30 22:33:32	Reading Code Signing Certificate	OK
2025-08-30 22:33:33	Running APKiD 2.1.5	OK
2025-08-30 22:33:37	Detecting Trackers	OK

2025-08-30 22:33:38	Decompiling APK to Java with JADX	OK
2025-08-30 22:33:49	Converting DEX to Smali	OK
2025-08-30 22:33:49	Code Analysis Started on - java_source	OK
2025-08-30 22:33:50	Android SBOM Analysis Completed	OK
2025-08-30 22:33:56	Android SAST Completed	OK
2025-08-30 22:33:56	Android API Analysis Started	OK
2025-08-30 22:34:02	Android API Analysis Completed	OK
2025-08-30 22:34:03	Android Permission Mapping Started	OK
2025-08-30 22:34:08	Android Permission Mapping Completed	OK
2025-08-30 22:34:08	Android Behaviour Analysis Started	OK
2025-08-30 22:34:14	Android Behaviour Analysis Completed	OK

2025-08-30 22:34:14	Extracting Emails and URLs from Source Code	OK
2025-08-30 22:34:15	Email and URL Extraction Completed	OK
2025-08-30 22:34:15	Extracting String data from APK	OK
2025-08-30 22:34:15	Extracting String data from Code	OK
2025-08-30 22:34:15	Extracting String values and entropies from Code	OK
2025-08-30 22:34:16	Performing Malware check on extracted domains	OK
2025-08-30 22:34:17	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.