ANDROID STATIC ANALYSIS REPORT

Android Auto (6.5)

File Name:	appv2.apk
Package Name:	com.system.task
Scan Date:	Aug. 10, 2024, 10:30 p.m.

App Security Score:	45/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	5/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
7	35	1	2	2

FILE INFORMATION

File Name: appv2.apk
Size: 6.97MB
MD5: 007a636ff170d63c523fbf01df3b0d78
SHA1: 751783df6723199b05616ad3a1d102e6acecedd9
SHA256: b998abf6914430ef879dcacfffe73c99573700fce0211ce2775c449f0f388a39

APP INFORMATION

App Name: Android Auto
Package Name: com.system.task
Main Activity: com.system.task.ActivationActivity
Target SDK: 26
Min SDK: 14
Max SDK:
Android Version Name: 6.5
Android Version Code:

APP COMPONENTS

Activities: 19
Services: 19
Receivers: 12
Providers: 2
Exported Activities: 5
Exported Services: 10
Exported Receivers: 8
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2017-11-15 12:50:57+00:00
Valid To: 2045-04-02 12:50:57+00:00
Issuer: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
Serial Number: 0x3a8ab0c4
Hash Algorithm: sha256
md5: f32c65511a7b0a47e09b254441355201

sha1: c276c3b087207c9d3ceeda766c01e0bdef7eac71
sha256: 28cc262edcb83b82b0c5da192d3ffd938ffaae163b44cdc528a6725de09de395
sha512: a141f98a23dc7ae94ce2c42790dcc839057e0984e7e56f1234b88f1d2722d4e0b2743b34123e4cda5ee10f80005319dae1428bfe398e1f5f13bf2d6f75dbab50
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 9f9f73c3802e28a6de107d2a16c088fd60630e6068fb0f83930edaf1ca26e9cd
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	normal	permission for using Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.	Permission an application must hold in order to use Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
android.permission.RESTART_PACKAGES	normal	kill background processes	Allows an application to kill background processes of other applications, even if memory is not low.
android.permission.KILL_BACKGROUND_PROCESSES	normal	kill background processes	Allows an application to kill background processes of other applications, even if memory is not low.
android.permission.GET_TASKS	dangerous	retrieve running applications	Allows application to retrieve information about currently and recently running tasks. May allow malicious applications to discover private information about other applications.
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_SMS	dangerous	read SMS or MMS	Allows application to read SMS messages stored on your phone or SIM card. Malicious applications may read your confidential messages.
android.permission.WRITE_SMS	dangerous	edit SMS or MMS	Allows application to write to SMS messages stored on your phone or SIM card. Malicious applications may delete your messages.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.RECEIVE_SMS	dangerous	receive SMS	Allows application to receive and process SMS messages. Malicious applications may monitor your messages or delete them without showing them to you.
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.DISABLE_KEYGUARD	normal	disable keyguard	Allows applications to disable the keyguard if it is not secure.
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.WRITE_CONTACTS	dangerous	write contact data	Allows an application to modify the contact (address) data stored on your phone. Malicious applications can use this to erase or modify your contact data.
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.PROCESS_OUTGOING_CALLS	dangerous	intercept outgoing calls	Allows application to process outgoing calls and change the number to be dialled. Malicious applications may monitor, redirect or prevent outgoing calls.
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.
com.android.browser.permission.READ_HISTORY_BOOKMARKS	unknown	Unknown permission	Unknown permission from android reference
android.permission.READ_CALENDAR	dangerous	read calendar events	Allows an application to read all of the calendar events stored on your phone. Malicious applications can use this to send your calendar events to other people.
com.google.android.gm.permission.READ_GMAIL	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.BATTERY_STATS	signature	modify battery statistics	Allows the modification of collected battery statistics. Not for use by common applications.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.READ_OWNER_DATA	unknown	Unknown permission	Unknown permission from android reference
android.permission.REAL_GET_TASKS	unknown	Unknown permission	Unknown permission from android reference
android.permission.PACKAGE_USAGE_STATS	signature	update component usage statistics	Allows the modification of collected component usage statistics. Not for use by common applications.
android.permission.SEND_SMS	dangerous	send SMS messages	Allows application to send SMS messages. Malicious applications may cost you money by sending messages without your confirmation.
android.permission.WRITE_INTERNAL_STORAGE	unknown	Unknown permission	Unknown permission from android reference
android.permission.WRITE_SETTINGS	dangerous	modify global system settings	Allows an application to modify the system's settings data. Malicious applications can corrupt your system's configuration.
android.permission.READ_CALL_LOG	dangerous	grants read access to the user's call log.	Allows an application to read the user's call log.
android.permission.WRITE_CALL_LOG	dangerous	allows writing to (but not reading) the user's call log.	Allows an application to write (but not read) the user's call log data.
android.permission.CHANGE_WIFI_STATE	normal	change Wi-Fi status	Allows an application to connect to and disconnect from Wi-Fi access points and to make changes to configured Wi-Fi networks.
android.permission.WRITE_SECURE_SETTINGS	SignatureOrSystem	modify secure system settings	Allows an application to modify the system's secure settings data. Not for use by common applications.
com.system.task.googlemapsv2.permission.MAPS_RECEIVE	unknown	Unknown permission	Unknown permission from android reference
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.ACCESS_SUPERUSER	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
com.system.task.permission.C2D_MESSAGE	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.MODEL check
Build.MANUFACTURER check
Build.BRAND check
Build.DEVICE check
Build.PRODUCT check
Build.TAGS check
network operator name check
possible VM check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>dx</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
possible Build.SERIAL check
Build.TAGS check
network operator name check</td></tr>
<tr><td>Compiler</td><td>dx</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.google.android.gms.tagmanager.TagManagerPreviewActivity	Schemes: tagmanager.c.com.system.task://,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

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: **4** | WARNING: **26** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 4.0-4.0.2, [minSdk=14]	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	Debug Enabled For App [android:debuggable=true]	high	Debugging was enabled on the app which makes it easier for reverse engineers to hook a debugger to it. This allows dumping a stack trace and accessing debugging helper classes.
3	Activity (com.system.task.ui.LockScreen) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.
4	Service (com.system.task.services.ZTIService) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
5	Service (com.system.task.services.MyFirebaseMessagingService) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Service is explicitly exported.
6	Service (com.system.task.services.MyFirebaseInstanceIDService) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Service is explicitly exported.
7	Broadcast Receiver (com.system.task.receivers.AndroidBroadcastReceiver) 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.
8	Broadcast Receiver (com.system.task.receivers.ServiceAlarmReceiver) 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.
9	Broadcast Receiver (com.system.task.receivers.AndroidTelephonyReceiver) 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.
10	Broadcast Receiver (com.system.task.receivers.AndroidScreenOnOffReceiver) 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.
11	Broadcast Receiver (com.system.task.receivers.EnterpriseDeviceAdminReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_DEVICE_ADMIN [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.
12	Broadcast Receiver (com.system.task.receivers.PackageChangeReceiver) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
13	Service (com.system.task.accessibility.SystemAccessibilityService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_ACCESSIBILITY_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.
14	Activity (com.system.task.ui.CustomActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.
15	Service (com.system.task.services.ScreenShotNonRootedService) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
16	Service (com.system.task.services.NotificationService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_NOTIFICATION_LISTENER_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.
17	Activity (com.google.android.gms.appinvite.PreviewActivity) is vulnerable to StrandHogg 2.0	high	Activity is found to be vulnerable to StrandHogg 2.0 task hijacking vulnerability. When vulnerable, it is possible for other applications to place a malicious activity on top of the activity stack of the vulnerable application. This makes the application an easy target for phishing attacks. The vulnerability can be remediated by setting the launch mode attribute to "singleInstance" and by setting an empty taskAffinity (taskAffinity=""). You can also update the target SDK version (26) of the app to 29 or higher to fix this issue at platform level.
18	Activity (com.google.android.gms.appinvite.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.
19	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [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.
20	Launch Mode of activity (com.google.firebase.auth.internal.FederatedSignInActivity) is not standard.	warning	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
21	Activity (com.google.firebase.auth.internal.FederatedSignInActivity) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.firebase.auth.api.gms.permission.LAUNCH_FEDERATED_SIGN_IN [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. 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.
22	Activity (com.google.android.gms.tagmanager.TagManagerPreviewActivity) is vulnerable to StrandHogg 2.0	high	Activity is found to be vulnerable to StrandHogg 2.0 task hijacking vulnerability. When vulnerable, it is possible for other applications to place a malicious activity on top of the activity stack of the vulnerable application. This makes the application an easy target for phishing attacks. The vulnerability can be remediated by setting the launch mode attribute to "singleInstance" and by setting an empty taskAffinity (taskAffinity=""). You can also update the target SDK version (26) of the app to 29 or higher to fix this issue at platform level.
23	Activity (com.google.android.gms.tagmanager.TagManagerPreviewActivity) 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.
24	Service (com.google.firebase.messaging.FirebaseMessagingService) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
25	Service (com.firebase.jobdispatcher.GooglePlayReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.permission.BIND_NETWORK_TASK_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.
26	Broadcast Receiver (com.google.android.gms.measurement.AppMeasurementInstallReferrerReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.INSTALL_PACKAGES [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.
27	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.
28	Service (com.google.firebase.iid.FirebaseInstanceIdService) 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.
29	High Intent Priority (999) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.
30	High Intent Priority (999) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.

CODE ANALYSIS

HIGH: **2** | WARNING: **7** | INFO: **1** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/firebase/jobdispatcher/ExecutionDelegator.java com/firebase/jobdispatcher/GooglePlayCallbackExtractor.java com/firebase/jobdispatcher/GooglePlayMessageHandler.java com/firebase/jobdispatcher/GooglePlayReceiver.java com/firebase/jobdispatcher/JobCoder.java com/firebase/jobdispatcher/JobService.java com/firebase/jobdispatcher/JobServiceConnection.java com/system/task/ActivationActivity.java

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	com/system/task/accessibility/AccessibilityManager.java com/system/task/accessibility/BrowserParser.java com/system/task/accessibility/NotificationLogManager.java com/system/task/accessibility/NotificationsNew.java com/system/task/accessibility/SystemAccessibilityService.java com/system/task/manager/AppWatcherManager.java com/system/task/manager/CallLogManager.java com/system/task/manager/ContactAPISdk5.java com/system/task/manager/DeviceStatusManager.java com/system/task/manager/FileSearchManager.java com/system/task/manager/FileUploadManager.java com/system/task/manager/GCMCommandManager.java com/system/task/manager/GeoFenceManager.java com/system/task/manager/InstallAppManager.java com/system/task/manager/InstalledAppPreferenceManager.java com/system/task/manager/ModulePreferencesManager.java com/system/task/manager/PendingCommandManager.java com/system/task/manager/PhotoManager.java com/system/task/manager/RegistrationManager.java com/system/task/manager/SMSLogManager.java com/system/task/manager/SchedulerManager.java com/system/task/manager/ScreenShootsManager.java com/system/task/manager/VideoManager.java com/system/task/manager/WifiLogManager.java com/system/task/manager/WifiReceiver.java com/system/task/network/HttpClient.java com/system/task/network/HttpManager.java com/system/task/persistence/DatabaseManager.java com/system/task/root/manager/ScreenRecordManager.java com/system/task/root/manager/TelegramManager.java com/system/task/root/manager/ViberCallManager.java com/system/task/services/MyFirebaseInstanceIDService.java com/system/task/services/NotificationService.java com/system/task/services/ScreenShotNonRootedService.java com/system/task/services/ZTIService.java com/system/task/ui/ActivationFragment.java com/system/task/ui/permission/PermissionActivity.java com/system/task/ui/permission/PermissionUtils.java com/system/task/utils/CommonUtils.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	com/system/task/utils/DateUtil.java com/system/task/utils/FileHelper.java com/system/task/utils/Logging.java com/system/task/persistence/DataBaseConnectionPool.java com/system/task/persistence/DatabaseManager.java com/system/task/root/manager/FacebookManager.java com/system/task/root/manager/GmailManager.java com/system/task/root/manager/KikManager.java com/system/task/root/manager/LineManager.java com/system/task/root/manager/SkypeManager.java com/system/task/root/manager/TelegramManager.java com/system/task/root/manager/TinderManager.java com/system/task/root/manager/ViberCallManager.java com/system/task/root/manager/ViberMessageManager.java com/system/task/root/manager/WhatsAppCallManager.java com/system/task/root/manager/WhatsAppManager.java
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/system/task/root/manager/FacebookManager.java com/system/task/utils/Constants.java com/system/task/utils/Recorder.java
4	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/system/task/manager/AppUpdateManager.java com/system/task/manager/ScreenShootsManager.java com/system/task/root/AppRootUtility.java com/system/task/root/manager/SkypeManager.java com/system/task/services/IntentServicesForOneTimeTasks.java com/system/task/services/ScreenShotNonRootedService.java com/system/task/utils/AppUtility.java com/system/task/utils/ClientGZipContentCompression.java com/system/task/utils/FileHelper.java com/system/task/utils/LoggingToServer.java com/system/task/utils/Recorder.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/system/task/manager/PushNotificationManager.java com/system/task/root/manager/ScreenRecordManager.java com/system/task/services/ScreenShotNonRootedService.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
6	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/system/task/root/RootedDataBase.java com/system/task/root/manager/SkypeManager.java com/system/task/utils/Recorder.java
7	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/system/task/manager/RegistrationManager.java
8	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/system/task/network/HttpManager.java
9	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/system/task/network/HttpManager.java
10	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/system/task/root/manager/ScreenRecordManager.java
11	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	com/system/task/root/AppRootUtility.java
12	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	com/system/task/BuildConfig.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	18/24	android.permission.GET_ACCOUNTS, android.permission.WAKE_LOCK, android.permission.GET_TASKS, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.READ_SMS, android.permission.RECEIVE_SMS, android.permission.ACCESS_FINE_LOCATION, android.permission.READ_CONTACTS, android.permission.READ_PHONE_STATE, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.RECORD_AUDIO, android.permission.VIBRATE, android.permission.SEND_SMS, android.permission.WRITE_SETTINGS, android.permission.READ_CALL_LOG, android.permission.INTERNET, android.permission.WRITE_EXTERNAL_STORAGE

TYPE	MATCHES	PERMISSIONS
Other Common Permissions	11/45	android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS, com.google.android.c2dm.permission.RECEIVE, android.permission.WRITE_SMS, android.permission.WRITE_CONTACTS, android.permission.CALL_PHONE, android.permission.PROCESS_OUTGOING_CALLS, android.permission.READ_CALENDAR, android.permission.BATTERY_STATS, android.permission.PACKAGE_USAGE_STATS, android.permission.CHANGE_WIFI_STATE, android.permission.ACCESS_SUPERUSER

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
alert.xiz4me.com	ok	**IP:** 84.22.120.16 **Country:** Netherlands **Region:** Zeeland **City:** Goes **Latitude:** 51.504169 **Longitude:** 3.888890 **View:** Google Map
sync.xiz4me.com	ok	**IP:** 84.22.120.16 **Country:** Netherlands **Region:** Zeeland **City:** Goes **Latitude:** 51.504169 **Longitude:** 3.888890 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
asset.xiz4me.com	ok	**IP:** 84.22.120.16 **Country:** Netherlands **Region:** Zeeland **City:** Goes **Latitude:** 51.504169 **Longitude:** 3.888890 **View:** Google Map
192.168.0.5	ok	**IP:** 192.168.0.5 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
xnspy.com	ok	**IP:** 104.26.8.182 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.mydwnd.com	ok	**IP:** 84.22.105.199 **Country:** Netherlands **Region:** Zeeland **City:** Goes **Latitude:** 51.504169 **Longitude:** 3.888890 **View:** Google Map
brilliant-flame-585.firebaseio.com	ok	**IP:** 35.190.39.113 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://brilliant-flame-585.firebaseio.com	info App talks to a Firebase Database.

TRACKERS

TRACKER	CATEGORIES	URL
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Google Tag Manager	Analytics	https://reports.exodus-privacy.eu.org/trackers/105

HARDCODED SECRETS

POSSIBLE SECRETS
"firebase_database_url" : "https://brilliant-flame-585.firebaseio.com"
"google_api_key" : "AIzaSyBTe9GAn6ZxhfjQJao2vEnUMaMqF6wcfFo"
"google_crash_reporting_api_key" : "AIzaSyBTe9GAn6ZxhfjQJao2vEnUMaMqF6wcfFo"
V/2NrZQU5cdFMpqYa0Q9vKRizJ0aHS7vWXQS8vp0qlI=
6qQh+8GAMu6fM86JkRzoeHiiHD67+MgHO4xhhwcbyPT7CQmAN57q8YytJQRqDjU5
notQcG55r2oh2A1cS/dLfKg9hawk3H86BF0iXzU7AAnhYpfHWl9mq3lZzdkAltxm
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
SFchXCfZXuuDAwXfTJDosXRUHrZZ0v26SJChYX3rL/o=

POSSIBLE SECRETS
115792089210356248762697446949407573530086143415290314195533631308867097853951
8Hx2xRqW2QZDPiXj7EKgQgzecg5taNOrZe4YkZ9zi7FcQAOy1BO0rYbAdBI9x6Pm
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
igTfSDGbP3Q2KSYfnqAL0vFW/zSSX6v+f+5s7NdwuKQgo6M7dQVerLATgNETrLAr
AIzaSyDRKQ9d6kfsoZT2lUnZcZnBYvH69HExNPE
JgKAyQW0PWqOrZHk4ZNT0IJH02FdSWTXOOjBnF9RRok=
cINMMi7uKicDN2DHSf1rHdgax7DU+CM2mIG3cRQw3SI0nkdhPwdVz1PCbewJpJoO
BiRNVQ0aQHyQJTXKNLbpSFJJy6+rG5ICwTiWxRhS6qdZjM6S9BBOaVfdO1b0Kd8E
B3EEABB8EE11C2BE770B684D95219ECB
I8ATAvvv3zdNeDvmT5gQ/ekfiNEF+bBdZZ3FGipPSiGHOLI4yQdK3XpX6xFRuejz
470fa2b4ae81cd56ecbcda9735803434cec591fa
FCjXGcebz7gnog9LMAWyd/isayIV3I84uK1cUtHZ2fI=
yzGxsS8IwfgINPYaD3TFRjRVH+0Pq4QvVGq15MBf/opCBPnlCr4QHvEcReKXEMs7
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
VWQmr3p+wsDJ15H20t2tLb975qLEArv8gtHgpBQKEOE=
DGPkHpN6F5DQjFiQDfOpLUfwAMooIPhSFT4YA2aSEj+k+u5Kt4pQoimNrK0aCsHP
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
ZsnUMRH5gS7aUE0TqnSYS8JWwJCKCL7bH7XFSqbI4dWEEyg2o14AuyyBvtsnwc4D
1Kj5K8xXQ2YA9zbG2Rm9FzZtUD9R2drVmZXzLVF7uLA=
Qplw2pUqnSpmThNy4cjVdvqrjxx/9Z0jyK1w8BPQVMfA35eh0MC7cXEA3u5Xkcuj
XxfDY0AzBkt4iSC5Sim2fww10jQc1evowDldz5+caY4=

POSSIBLE SECRETS
SRWP8PeqaQflId3WUP9WJTho9Un3bF1tLB8c7UP1Ruo=
2GI4cQuNT2V9TGPC/Z2McvgqRAU80qquJKbm0BMTxLR8WwMEgJwPEKdGCxKNxeUN
HYkEKMk8dvMdQrlbFR00sh73U7jSOxxrrxd0BhHmEXYlIfEqe1EzBQsw2kucbDs8
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
5XuSFVTSxDkE27CIZHrBIXal5K53Dv1J/UFXKGBFAXY=
Wz4eX479PrQ8rGu0gkJoEYqOJ2Dr8sAHE85KoBBz7s4=
115792089210356248762697446949407573529996955224135760342422259061068512044369
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
yATd8qneW4MlwQIx8jIN6cfiWJ28/zOw6vW7xs0IWvNvim2a85v5X4ZiVD1KK9hX
oWVj3eW9lsJMixyFq7g0kyuRqYP087mdDp4dCL3paE/7Ut3Ewp3IcEq6P10MPRyy
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
pdXBsPFh4N2rQp3r0gjTSQiWtas1GOGaKulNSciQTj0=
Z7StFiuQ59x4y88apmlBJn3lPoWOEnuqoEhP2AVUL8A=
wM87KVhGHShMaqkZWTxt04VnU6kJHrMxqQyksEW6glI=
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
WKdn2zzE+pFOb2FrixdUDF+m9GVRaxGTq2U3/uOmGmE=
U9ntf5BvZUTabci6TosC4bQNHZ+DOrzvRmpSy4CzkoQ=
peD/v7hHRn46N2uI0dQKpTtMr7rKDQ+Rzb4yluPWMw4TUUwj2SFV9GkdTp0kog66
0wjmexcQnona3bxO7Nd7FrKMEEoBhOp7s6KivBhMQKU=
siNRngHYHRLjixmg2PEX5OdKhRHe1h8DNRpJp4wC0pk=

POSSIBLE SECRETS
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
2glehmg5UKxyaNPdnG06BLa5QbEzBADKVm3lYiT3+JTkguRZEzOA9BDahqC4W8ki
Qrc1hPZgr+QjlmQtpbdJO1QCxqr2PdTRKIIDeDNdHp8=
z9Ycw/7CJTzBzg6MPXNZ2oLMXcxWzT8qsF0ig0ITUxc=
VywbbfxE2QuRqZ5xcIwapO7AdSzfVaSWnmJxmUg+0adJ3QBAH5P7EgXr1uzyY+u6
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319
4w5pMN4cUsuXvD3CJ7PKPSwMmWPClIaNSjeM6jtHahV40Q7EiLps1VIbOcEaCSp4
HBbZPURZUWU/TDYIx99LmOTdgpFP2mdidp6Zk4sZdEVCGaQNYtmNlQBCP3rgXOne
nJw4XP5tQfSQ6wm+0x6UMq5j2kNiUh+TXa92gyyhaOo=
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
39402006196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643

SCAN LOGS

Timestamp	Event	Error
2024-08-10 22:30:54	Generating Hashes	OK
2024-08-10 22:30:54	Extracting APK	OK
2024-08-10 22:30:54	Unzipping	OK
2024-08-10 22:30:54	Getting Hardcoded Certificates/Keystores	OK

2024-08-10 22:30:56	Parsing AndroidManifest.xml	OK
2024-08-10 22:30:56	Parsing APK with androguard	OK
2024-08-10 22:30:57	Extracting Manifest Data	OK
2024-08-10 22:30:57	Performing Static Analysis on: Android Auto (com.system.task)	OK
2024-08-10 22:30:57	Fetching Details from Play Store: com.system.task	OK
2024-08-10 22:30:57	Manifest Analysis Started	OK
2024-08-10 22:30:57	Checking for Malware Permissions	OK
2024-08-10 22:30:57	Fetching icon path	OK
2024-08-10 22:30:57	Library Binary Analysis Started	OK
2024-08-10 22:30:57	Reading Code Signing Certificate	OK
2024-08-10 22:30:57	Running APKiD 2.1.5	OK
2024-08-10 22:30:59	Detecting Trackers	OK
2024-08-10 22:31:00	Decompiling APK to Java with jadx	OK
2024-08-10 22:31:14	Converting DEX to Smali	OK

2024-08-10 22:31:14	Code Analysis Started on - java_source	OK
2024-08-10 22:31:19	Android SAST Completed	OK
2024-08-10 22:31:19	Android API Analysis Started	OK
2024-08-10 22:31:22	Android Permission Mapping Started	OK
2024-08-10 22:31:33	Android Permission Mapping Completed	OK
2024-08-10 22:31:33	Finished Code Analysis, Email and URL Extraction	OK
2024-08-10 22:31:33	Extracting String data from APK	OK
2024-08-10 22:31:34	Extracting String data from Code	OK
2024-08-10 22:31:34	Extracting String values and entropies from Code	OK
2024-08-10 22:31:35	Performing Malware check on extracted domains	OK
2024-08-10 22:31:36	Saving to Database	OK

Report Generated by - MobSF v4.0.6

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.