MOBSF

ANDROID STATIC ANALYSIS REPORT

Sync Service (7.5.369)

File Name:	setup-r856.apk
Package Name:	com.android.core.mntan
Scan Date:	Aug. 10, 2024, 6:50 p.m.

App Security Score: 51/100 (MEDIUM RISK)

Grade: B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	27	1	2	1

FILE INFORMATION

File Name: setup-r856.apk
Size: 2.12MB
MD5: 61a77fa18e59947d923e8e6dc8569ace
SHA1: 6ecdcc3d6d345280c5df8176cdb18077e0e3ef69
SHA256: 49eb2fb7f5968909c06d75d71cf8be0849038e213fddbc1e899c835367c63b50

APP INFORMATION

App Name: Sync Service
Package Name: com.android.core.mntan
Main Activity: com.activities.ActivityMainStarter
Target SDK: 33
Min SDK: 19
Max SDK:
Android Version Name: 7.5.369
Android Version Code: 369

APP COMPONENTS

Activities: 8
Services: 5
Receivers: 9
Providers: 2
Exported Activities: 7
Exported Services: 5
Exported Receivers: 9
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: False
v3 signature: False
v4 signature: False
X.509 Subject: O=H20240626
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2024-06-25 22:40:55+00:00
Valid To: 2049-06-19 22:40:55+00:00
Issuer: O=H20240626
Serial Number: 0x7151ceb5
Hash Algorithm: sha256
md5: 21bce8e74354bc9bcf556d6a9fa96758
sha1: b7a46574ba26268bf77275a38c31aac6723a29d4
sha256: 3206994639eb0d9b90f75ee394e3f7f7938cc490b9d3e726fd36ffb47c92939b

sha512: d1ba8947629824b5a2aa4e91ec5792936754e90ccf9c1e0b8c3d073ef201cf82e1eb0090700c5812c0a1b7600128c1c0af8a5a5fb658dbdeb8eca7ff863471fc
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 65a8869c8b0410709e2451ee1de5673b098ce3899fcee4732e68fc55bd3486b5
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
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_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background.
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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.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.READ_CALENDAR	dangerous	read calendar events	Allows an application to read all of the calendar events stored on your phone. Malicious applications can use this to send your calendar events to other people.
android.permission.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.

PERMISSION	STATUS	INFO	DESCRIPTION
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.READ_PHONE_NUMBERS	dangerous	allows reading of the device's phone number(s).	Allows read access to the device's phone number(s). This is a subset of the capabilities granted by READ_PHONE_STATE but is exposed to instant applications.
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.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.READ_PRIVILEGED_PHONE_STATE	unknown	Unknown permission	Unknown permission from android reference
android.permission.READ_LOGS	dangerous	read sensitive log data	Allows an application to read from the system's various log files. This allows it to discover general information about what you are doing with the phone, potentially including personal or private information.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.MANAGE_EXTERNAL_STORAGE	dangerous	Allows an application a broad access to external storage in scoped storage	Allows an application a broad access to external storage in scoped storage. Intended to be used by few apps that need to manage files on behalf of the users.
android.permission.PACKAGE_USAGE_STATS	signature	update component usage statistics	Allows the modification of collected component usage statistics. Not for use by common applications.
com.android.browser.permission.READ_HISTORY_BOOKMARKS	unknown	Unknown permission	Unknown permission from android reference
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
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.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.REQUEST_INSTALL_PACKAGES	dangerous	Allows an application to request installing packages.	Malicious applications can use this to try and trick users into installing additional malicious packages.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.INTERACT_ACROSS_USERS	unknown	Unknown permission	Unknown permission from android reference
android.permission.INTERACT_ACROSS_USERS_FULL	unknown	Unknown permission	Unknown permission from android reference
android.permission.REQUEST_DELETE_PACKAGES	normal	enables an app to request package deletions.	Allows an application to request deleting packages.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.QUERY_ALL_PACKAGES	normal	enables querying any normal app on the device.	Allows query of any normal app on the device, regardless of manifest declarations.
android.permission.BLUETOOTH_CONNECT	dangerous	necessary for connecting to paired Bluetooth devices.	Required to be able to connect to paired Bluetooth devices.
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.
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.SYSTEM_ALERT_WINDOW	dangerous	display system-level alerts	Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.

PERMISSION	STATUS	INFO	DESCRIPTION
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.

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Anti-VM Code — DETAILS: Build.MANUFACTURER check possible Build.SERIAL check SIM operator check network operator name check FINDINGS: Compiler — DETAILS: unknown (please file detection issue!)

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 0 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate

MANIFEST ANALYSIS

HIGH: 1 | WARNING: 23 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 4.4-4.4.4, [minSdk=19]	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	Activity (com.activities.ActivityDblStarter) 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.
3	Activity (com.activities.ActivityMain) 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.
4	Launch Mode of activity (com.activities.ActivityTrScr) 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.
5	Activity (com.activities.ActivityTrScr) 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.
6	Service (hw.utils.ServiceCore) 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.
7	Service (hw.recorder.ServiceRecording) 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.
8	Service (hw.utils.ServiceScr) 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.
9	Broadcast Receiver (com.utils.receivers.ReceiverChangeConnection) 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.utils.receivers.ReceiverOutgoingCall) 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.utils.receivers.ReceiverBoot) 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.
12	Broadcast Receiver (com.utils.receivers.ReceiverUserPresent) 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
13	Broadcast Receiver (hw.core.ReceiverAlarm) 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.
14	Broadcast Receiver (hw.recorder.ReceiverMsg) 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.
15	Activity (com.activities.ActivityWidget) 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.
16	Broadcast Receiver (com.utils.widgets.WidgetProvider) 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.
17	Broadcast Receiver (com.utils.receivers.ReceiverPowerEvents) 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.
18	Broadcast Receiver (com.utils.receivers.ReceiverAirplaneMode) 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.
19	Activity (hw.installer.ActivityInstaller) 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.
20	Activity (hw.installer.ReaderServiceCheckerActivity) 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.
21	Activity (hw.installer.ScreenshotCheckerActivity) 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.
22	Service (hw.imreader.ReaderAccessibilityService) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
23	Service (hw.imreader.ReaderNotificationService) 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.
24	High Intent Priority (2147483646) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.

</> CODE ANALYSIS

HIGH: **1** | WARNING: **3** | INFO: **1** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES

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	b/a/k/a/a.java b/a/m/g.java b/g/d/b.java b/g/d/e.java b/g/d/f.java b/g/d/i.java b/g/j/b.java b/g/k/b.java b/g/k/e.java b/g/k/g.java b/g/k/r.java b/g/k/t.java b/i/b/a.java b/j/a/a.java b/j/a/b.java b/j/a/e.java b/j/a/j.java b/j/a/m.java b/l/a/b.java b/l/b/c.java b/n/d0.java b/n/e0.java b/n/f0.java b/n/g0.java b/n/y.java b/n/z.java b/o/a/a/h.java c/b/a/a/j/h.java c/b/a/a/k/a.java com/utils/core/CoreApplication.java hw/installer/FragmentInstallLogin.java hw/installer/ReaderServiceCheckerActivity.java hw/utils/l.java hw/utils/m.java
2	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	hw/database/h.java hw/imreader/h.java hw/utils/o.java hw/utils/r.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	c/c/c/b.java c/c/c/d.java c/c/c/i.java hw/database/b.java hw/database/h.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	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	d/a/a/a/f/d/k.java
5	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	e/a/a.java e/a/b.java
6	Weak Encryption algorithm used	high	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	hw/utils/h.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	20/24	android.permission.RECEIVE_SMS, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.READ_CONTACTS, android.permission.READ_SMS, android.permission.READ_CALL_LOG, android.permission.READ_PHONE_STATE, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.INTERNET, android.permission.GET_TASKS, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.RECORD_AUDIO, android.permission.WAKE_LOCK, android.permission.CAMERA, android.permission.GET_ACCOUNTS, android.permission.WRITE_SETTINGS, android.permission.SYSTEM_ALERT_WINDOW
Other Common Permissions	9/45	android.permission.ACCESS_BACKGROUND_LOCATION, android.permission.READ_CALENDAR, android.permission.PROCESS_OUTGOING_CALLS, android.permission.PACKAGE_USAGE_STATS, android.permission.BLUETOOTH, android.permission.MODIFY_AUDIO_SETTINGS, android.permission.REQUEST_INSTALL_PACKAGES, android.permission.FOREGROUND_SERVICE, android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS

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
xmlpull.org	ok	**IP:** 185.199.110.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
www.google.com	ok	**IP:** 142.251.39.4 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

HARDCODED SECRETS

POSSIBLE SECRETS
lrH2Zm0JF+MdZcKkUKBf1Pv5W7uFbwla2XNHCjr2LTEcduvI7tFe8g==
0Uji2E/esiv4G0Mf1dQghVqVAqSyHaJX
O4MkUWSy2w8l+q9IeEEKmD8bzy/MLGOuO4MkUWSy2w8AGXZGDD1v7oP2Y7eJwWNb913z4+UPlNgQ
3fyV19Ubrzy0I8TMlynRaqHeVVP+T8kp
O4MkUWSy2w/J0RDFuayF5Ews4PV4Ocp8zP7SC0Tqr8tNqvR67gt5eLENzuZr371ILX3yaN+WuMUV
KCiTyJ1RfIhtFxFtjPmoopa89NVCKFvN

POSSIBLE SECRETS
no/m0ruse4stmDc+aPJ7hLX3yaN+WuMUKC5YLbFNtkA==
xLiWIG9WNxnXZVYDTGhrje6wnHt5vGXh

SCAN LOGS

Timestamp	Event	Error
2024-08-10 18:50:05	Generating Hashes	OK
2024-08-10 18:50:05	Extracting APK	OK
2024-08-10 18:50:05	Unzipping	OK
2024-08-10 18:50:05	Getting Hardcoded Certificates/Keystores	OK
2024-08-10 18:50:07	Parsing AndroidManifest.xml	OK
2024-08-10 18:50:07	Parsing APK with androguard	OK
2024-08-10 18:50:07	Extracting Manifest Data	OK
2024-08-10 18:50:07	Performing Static Analysis on: Sync Service (com.android.core.mntan)	OK
2024-08-10 18:50:07	Fetching Details from Play Store: com.android.core.mntan	OK

2024-08-10 18:50:08	Manifest Analysis Started	OK
2024-08-10 18:50:08	Checking for Malware Permissions	OK
2024-08-10 18:50:08	Fetching icon path	OK
2024-08-10 18:50:08	Library Binary Analysis Started	OK
2024-08-10 18:50:08	Reading Code Signing Certificate	OK
2024-08-10 18:50:08	Failed to get signature versions	CalledProcessError(1, ['/jdk-20.0.2/bin/java', '-Xmx1024M', '-Djava.library.path=', '-jar', '/home/mobsf/Mobile-Security-Framework-MobSF/mobsf/StaticAnalyzer/tools/apksigner.jar', 'verify', '--verbose', '/home/mobsf/.MobSF/uploads/61a77fa18e59947d923e8e6dc8569ace/61a77fa18e59947d923e8e6dc8569ace.apk'])
2024-08-10 18:50:08	Running APKiD 2.1.5	OK
2024-08-10 18:50:09	Detecting Trackers	OK
2024-08-10 18:50:10	Decompiling APK to Java with jadx	OK
2024-08-10 18:50:14	Converting DEX to Smali	OK
2024-08-10 18:50:14	Code Analysis Started on - java_source	OK
2024-08-10 18:50:18	Android SAST Completed	OK
2024-08-10 18:50:18	Android API Analysis Started	OK

2024-08-10 18:50:21	Android Permission Mapping Started	OK
2024-08-10 18:50:34	Android Permission Mapping Completed	OK
2024-08-10 18:50:34	Finished Code Analysis, Email and URL Extraction	OK
2024-08-10 18:50:34	Extracting String data from APK	OK
2024-08-10 18:50:34	Extracting String data from Code	OK
2024-08-10 18:50:34	Extracting String values and entropies from Code	OK
2024-08-10 18:50:34	Performing Malware check on extracted domains	OK
2024-08-10 18:50:36	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.