ANDROID STATIC ANALYSIS REPORT

Poczta (1.0)

File Name:	fefd353bac6e06b45a4593b22a03b57b3b1d28c25edde151ace8dee06fadd9ac.apk
Package Name:	tgffsznnfaqz.uigqoxhqdhzw.stijcdihrnxemufcckfnwskrgta
Average CVSS Score:	5.7
App Security Score:	75/100 (LOW RISK)
Trackers Detection:	2/285

FILE INFORMATION

File Name: fefd353bac6e06b45a4593b22a03b57b3b1d28c25edde151ace8dee06fadd9ac.apk
Size: 1.54MB
MD5: 1b75faf2adfc63ee8448b57bdf23d48e
SHA1: 3f72a4dd42cdf126e27dbd843847f0f3af39bf29
SHA256: fefd353bac6e06b45a4593b22a03b57b3b1d28c25edde151ace8dee06fadd9ac

APP INFORMATION

App Name: Poczta
Package Name: tgffsznnfaqz.uigqoxhqdhzw.stijcdihrnxemufcckfnwskrgta
Main Activity: sniaean.azaskhuucmmuid.okrk.bhzetnyubga
Target SDK: 29
Min SDK: 15
Max SDK:
Android Version Name: 1.0
Android Version Code: 1

APP COMPONENTS

Activities: 38
Services: 8
Receivers: 3
Providers: 0
Exported Activities: 1
Exported Services: 0
Exported Receivers: 0
Exported Providers: 0

CERTIFICATE INFORMATION

APK is signed
v1 signature: True
v2 signature: False
v3 signature: False
Found 1 unique certificates
Subject: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2008-02-29 01:33:46+00:00
Valid To: 2035-07-17 01:33:46+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
Serial Number: 0x936eacbe07f201df
Hash Algorithm: sha1
md5: e89b158e4bcf988ebd09eb83f5378e87
sha1: 61ed377e85d386a8dfee6b864bd85b0bfaa5af81
sha256: a40da80a59d170caa950cf15c18c454d47a39b26989d8b640ecd745ba71bf5dc
sha512:
5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccbe6b34ec4233f5f640703581053abfea303977272d17958704d89b7711292a4569

Certificate Status: Bad
Description: The app is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues.

☰ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.DISABLE_KEYGUARD	dangerous	disable key lock	Allows an application to disable the key lock and any associated password security. A legitimate example of this is the phone disabling the key lock when receiving an incoming phone call, then re-enabling the key lock when the call is finished.
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	normal		Permission an application must hold in order to use
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.CHANGE_WIFI_MULTICAST_STATE	dangerous	allow Wi-Fi Multicast reception	Allows an application to receive packets not directly addressed to your device. This can be useful when discovering services offered nearby. It uses more power than the non-multicast mode.
android.permission.WAKE_LOCK	dangerous	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.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.REORDER_TASKS	dangerous	reorder applications running	Allows an application to move tasks to the foreground and background. Malicious applications can force themselves to the front without your control.

PERMISSION	STATUS	INFO	DESCRIPTION
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.NFC	dangerous	control Near-Field Communication	Allows an application to communicate with Near-Field Communication (NFC) tags, cards and readers.
android.permission.INTERNET	dangerous	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.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.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.REQUEST_DELETE_PACKAGES	normal		Allows an application to request deleting packages. Apps targeting APIs

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>Compiler</td><td>dexlib 2.x</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
sniaean.azaskhuucmmuid.okrk.ckiwrpemditft	Schemes: sms://, mms://, mmsto://, smsto://,

MANIFEST ANALYSIS

ISSUE	SEVERITY	DESCRIPTION
Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
Application Data can be Backed up [android:allowBackup=true]	medium	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
Activity (sniaean.azaskhuucmmuid.okrk.ckiwrpemditft) is not Protected. An intent-filter exists.	high	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.
Launch Mode of Activity (sniaean.azaskhuucmmuid.okrk.ewqngluwcaqxzd.ofbzz) is not standard.	high	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.
High Intent Priority (121) [android:priority]	medium	By setting an intent priority higher than another intent, the app effectively overrides other requests.
High Intent Priority (979) [android:priority]	medium	By setting an intent priority higher than another intent, the app effectively overrides other requests.

CODE ANALYSIS

ISSUE	SEVERITY	STANDARDS	FILES
Files may contain hardcoded sensitive informations like usernames, passwords, keys etc.	high	**CVSS V2:** 7.4 (high) **CWE:** CWE-312 - Cleartext Storage of Sensitive Information **OWASP Top 10:** M9: Reverse Engineering **OWASP MASVS:** MSTG-STORAGE-14	ru/auto/ara/plugin/launch/DictionaryPlugin.java ru/auto/ara/plugin/launch/LogAppLaunchPlugin.java ru/auto/ara/data/preferences/DefaultPreferences.java com/adjust/sdk/sigv2/KeystoreHelper.java

ISSUE	SEVERITY	STANDARDS	FILES
The App logs information. Sensitive information should never be logged.	info	**CVSS V2:** 7.5 (high) **CWE:** CWE-532 - Insertion of Sensitive Information into Log File **OWASP MASVS:** MSTG-STORAGE-3	ru/auto/ara/utils/logger/SoftWrapDebugTree.java ru/yandex/searchlib/util/Log.java com/adjust/sdk/sigv2/Crypt.java com/bumptech/glide/Glide.java com/bumptech/glide/GeneratedAppGlideModuleImpl.java com/bumptech/glide/manager/c.java com/bumptech/glide/manager/h.java com/bumptech/glide/manager/d.java com/bumptech/glide/manager/i.java com/bumptech/glide/manager/j.java com/bumptech/glide/manager/RequestTracker.java com/bumptech/glide/request/d.java com/bumptech/glide/request/target/c.java com/bumptech/glide/request/target/ViewTarget.java
This App uses Java Hash Code. It's a weak hash function and should never be used in Secure Crypto Implementation.	warning	**CVSS V2:** 2.3 (low) **CWE:** CWE-327 - Use of a Broken or Risky Cryptographic Algorithm **OWASP MASVS:** MSTG-CRYPTO-4	ru/yandex/searchlib/informers/main/RatesInformerResponse.java ru/yandex/searchlib/json/HistoryStreamAdapter.java ru/yandex/searchlib/json/HomeApiJsonReaderMainInformersResponseJsonAdapter.java ru/yandex/searchlib/json/YandexJsonReaderNavigationResponseJsonAdapter.java ru/yandex/searchlib/json/MainActivityHistoryParser.java ru/yandex/searchlib/json/JsonReaderTrendResponseJsonAdapter.java ru/yandex/searchlib/history/HistoryItem.java com/annimon/stream/c.java com/flipboard/bottomsheet/commons/IntentPickerSheetView.java com/bumptech/glide/request/d.java

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
autoru-mag-data.s3.yandex.net	good	**IP:** 93.158.134.158 **Country:** Russian Federation **Region:** Moskva **City:** Moscow **Latitude:** 55.75222 **Longitude:** 37.615559 **View:** Google Map
m.auto.ru	good	**IP:** 213.180.204.188 **Country:** Russian Federation **Region:** Moskva **City:** Moscow **Latitude:** 55.75222 **Longitude:** 37.615559 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
m.test.avto.ru	good	**IP:** 213.180.193.188 **Country:** Russian Federation **Region:** Moskva **City:** Moscow **Latitude:** 55.75222 **Longitude:** 37.615559 **View:** Google Map
suggestions.dadata.ru	good	**IP:** 186.2.163.83 **Country:** Russian Federation **Region:** Rostovskaya oblast' **City:** Rostov-na-Donu **Latitude:** 47.23563 **Longitude:** 39.712189 **View:** Google Map
api.yastatic.net	good	**IP:** 178.154.131.215 **Country:** Russian Federation **Region:** Moskva **City:** Moscow **Latitude:** 55.75222 **Longitude:** 37.615559 **View:** Google Map

URLS

URL	FILE
https://suggestions.dadata.ru/ https://autoru-mag-data.s3.yandex.net/json/	ru/auto/ara/di/module/ApiModule.java
https://m.auto.ru/ http://m.auto.ru/ https://m.test.avto.ru/ http://m.test.avto.ru/	ru/auto/ara/utils/ServerChooseHelper.java
www.)?drive2	ru/auto/data/util/StringUtils.java
https://api.yastatic.net/morda-logo/i/yandex-app/weather/wgt_android/%s.4.png	ru/yandex/searchlib/informers/main/WeatherIconMapper.java

TRACKERS

TRACKER	URL
Adjust	https://reports.exodus-privacy.eu.org/trackers/52
AppMetrica	https://reports.exodus-privacy.eu.org/trackers/140

App Security Score Calculation

Every app is given an ideal score of 100 to begin with.
For every findings with severity high we reduce 15 from the score.
For every findings with severity warning we reduce 10 from the score.
For every findings with severity good we add 5 to the score.
If the calculated score is greater than 100, then the app security score is considered as 100.
And if the calculated score is less than 0, then the app security score is considered as 10.

Risk Calculation

APP SECURITY SCORE	RISK
0 - 15	CRITICAL
16 - 40	HIGH
41 - 70	MEDIUM
71 - 100	LOW

Report Generated by - MobSF v3.0.7 Beta

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.