Fraunhofer
SIT

Appicaptor Report

Results for Telecooperation Lab. TU Darmstadt

Fraunhofer Institute for
Secure Information Technology (SIT)

December 8, 2016

For internal use only!

„Investment in your Future“

Investments for this work were co-funded
by the European Union with European regional
development funds and by the state
government of Hessen

Fraunhofer SIT contact person
Dr. Jens Heider
Fraunhofer Institute for Secure Information Technology (SIT)
Rheinstraße 75, 64295 Darmstadt, Germany
Email: jens.heider@sit.fraunhofer.de
Phone: +49 (0) 61 51/869-233
Fax: +49 (0) 61 51/869-224

Contents

1 Terms of Use

The Results and accompanying information generated by Fraunhofer SIT and provided to the client are protected by copyright for Fraunhofer Gesellschaft e. V., all rights reserved. The Results will be provided to the client at Fraunhofer SIT' sole discretion and are be subject to strict confidentiality and use restrictions as detailed below as the Results - among others - contain benchmark test results with regard to third party software.

The client shall only be granted a non-exclusive, non-transferable, non-sublicensable right to use the Results for its own internal evaluation purposes only. The client shall not be entitled to release, transfer, assign, rent, lease, sell, disclose or otherwise publish the Results.

The client shall not be entitled to allow access to the Results - in whole or in part - or any information contained therein by any third party and shall be liable that its employees shall comply with the obligations above.

Each violation of the restrictions to use the Results as outlined above by the client shall be subject to damage claims and claims to refrain from any unauthorized use of the Results. In addition, the client shall indemnify Fraunhofer from any third party claim resulting from the client's violation of these obligations.

2 Overview

Appicaptor is a framework for semi-automated security testing of apps. Generated by the framework, this report represents an aggregated interpretation of the performed tests to answer questions about security and privacy related properties of apps.

The apps listed in Table 2.1 were selected by the customer to be tested with the Appicaptor Framework. For each app a test model was derived which describes the nature of the app best. The test model is used to configure tests and it provides information for correlating single test results to an overall result. A generic model is applied for apps that are not tagged for tests specific to a certain class of apps. The listed versions corresponds to the values specified in the app archives and may differ from those displayed in the app store if a developer had chosen to use a diffrent version string for the app store.

Table 2.1: Overview of tested apps, versions and applied test models

App Name	Version	OS	Test Model
1Weather: Wetter-App	4.0.1	Android	Weather
AccuWeather	4.3.7-free	Android	Weather
Drops - der Regenalarm	3.6.7	Android	Weather
Genaues Wetter für Deutschland	5.6.7	Android	Weather
GO Wetter Vorhersage& Widgets	5.733	Android	Weather
RainToday . HD Regenradar	1.5.1	Android	Weather
RegenRadar	3.12.5	Android	Weather
Thermometer++	2.5.2	Android	Weather
Transparent Clock & Wetter	0.92.01.07	Android	Weather
WarnWetter	1.5	Android	Weather
WeatherPro Free: Wetter gratis	1.3	Android	Weather
Wetter & Uhr-Widget - Android	5.9.1.2	Android	Weather
Wetter Deutschland XL PRO	1.4.0	Android	Weather
Wetter Live Kostenlos	5.1	Android	Weather
Wetter Radar Schnee MORECAST.	3.1.2	Android	Weather
Wetter und Radar - wetter.com	2.12.3	Android	Weather
Wetter.de - Regenradar & mehr	3.6.2	Android	Weather
wetter.info	1.7.7	Android	Weather
WetterOnline	3.14.3	Android	Weather
Wetter.Weather	1.4.12	Android	Weather

3 Results

The presented results are based on automated test procedures. All test metrics are carefully chosen and cross-checked. For stating a single app property, multiple independent tests are conducted and correlated to prevent incorrect results. Conflicting results or results that break specified assumptions are denoted by a question mark in the results to prevent false interpretation. Those potential ambiguous results are subject to further improvements of test procedures by integrating insights of manual investigations into improved tests.

Due to the nature of automated tests, however, the correctness of the presented results can not be guaranteed. The results are based on work created to the best of our knowledge and belief.

Table 3.1: Legend

☒	tested property was found
☒ *i*	tested property was found (see detail section for limitations)
☐	tested property was not found
☐ *i*	tested property was not found (see detail section for limitations)
☑	test created proper test results
⊟	test created no test results
?	test created conflicting results
⚡	error conditions during test

3.1 1Weather: Wetter-App (Android)

3.1.1 Tests

The following Table 3.2 summarizes the results of the Android app `1Weather: Wetter-App` with version *4.0.1*.

Table 3.2: Overview of summarized test results for »1Weather: Wetter-App«

App risks for enterprise usage	
☐	*Implementation flaws? No.*
☒	*Privacy risks? Yes.*
☒	*Security risks? Yes.*
Blacklisted by policy	
☐	*Violations of default policy? No.*
Communication security	

☒ *Client communication used? Yes.*
☑ *Communication endpoints: 68 entries, see details.*
☑ *Communication with country: 6 entries, see details.*
☒ *SSL/TLS used? Yes.*
☒ *Custom SSL/TLS trust manager implemented? Yes.*
☐ *Faulty custom SSL/TLS trust manager implemented? No.*
☒ *SSL/TLS using custom error handling? Yes.*
☐ *SSL/TLS using faulty custom error handling? No.*
☐ *SSL/TLS using manual domain name verification? No.*
☒ *Unprotected HTML? Yes.*
☒ *Unprotected JavaScripts? Yes.*
☒ *Unprotected communication? Yes.*

Data security

☑ *Cryptographic Primitives:* `"AES/CBC/PKCS5Padding", "AES/CBC/PKCS7Padding", "AES/ECB/PKCS7Padding", "RSA/ECB/PKCS1Padding"`
☒ *Cryptographic keys found? Yes.*
☒ *Application needs normal permissions? Yes.*
☒ *Application needs dangerous permissions? Yes.*
☑ *Userdefined permission usage: 6 entries, see details.*
☑ *Overprivileged permissions:* `READ_EXTERNAL_STORAGE`
☒ *Is application overprivileged? Yes.*
☒ *Application defines content provider? Yes.*
− *Content provider accessible without permission: None.*
☒ *JavaScript to SDK API bridge usage? Yes.*
☐ *WiFi-Direct enabled? No.*

Input interface security

− *App can handle documents of mimeType: None.*
☐ *Screenshot protection used? No.*
☐ *Tap Jacking Protection used? No.*

Privacy

☒ *Installed app list accessed? Yes.*
☒ *Obfuscation used? Yes.*
☑ *Obfuscation level is:* `UNKNOWN`
− *Device administration policy entries: None.*
☑ *Accessed unique identifier(s): 12 entries, see details.*
☑ *Advertisment-/tracking frameworks found: 6 entries, see details.*
☒ *App provides public accessible activities? Yes.*
☒ *Backup of app is allowed? Yes.*
☒ *Log Statement Enabled? Yes.*
☐ *Permission to access address book? No.*
☑ *Sensor usage:* `Camera (inactive), WIFI-Based Location, GPS Location, Acceleration/Light`

☒	*Unprotected preference files found? Yes.*
Runtime Security	
☒	*Scheduled Alarm Manager registered? Yes.*
☑	*Alarm repeating types:* `RTC-WAKEUP`
☒	*Alarm intervals dynamically? Yes.*
☐	*Alarm Manager initialized dynamically? No.*
☒	*Dynamically loaded code at runtime? Yes.*
☑	*Dynamically loaded code at runtime type(s):* `dalvik.system.DexClassLoader(...)`, `ClassLoader.loadClass(...)`, `loadLibrary(...)`
☐	*Allow app debugging Flag? No.*
☒	*App uses outdated signature key? Yes.*
☒	*Contains native libraries: Yes.*
☑	*Executed component after Phone Reboot:* `com.handmark.expressweather.BootReceiver`

3.1.2 Details

The following sections describe details about the test results of `1Weather: Wetter-App` with version *4.0.1*.

App risks for enterprise usage

- Reasons for category privacy risks:
  - Advertisement/Tracking: App uses more than 5 advertisement and tracking providers.
  - App tries to access the device phone number which can be use to identify the owner remotely.
  - App Listing: Usage of detected functionality to access list of installed apps poses a privacy risk for detected app type.
- Reasons for category security risks:
  - Unprotected Web Content: App loads active web content (e.g. JavaScript or HTML files) without integrity protection. This poses a risk as man-in-the-middle attackers can modify the loaded web content and change the functionality of the app.
  - Crypto: Embedded static encryption key found, which can be extracted by attackers to revert the encryption or fake the signature of the content it is used for.

Communication security

- Client communication detected. The application can establish a network connection to one or more specific host systems. URLs with parameters found:
  - `#KEEP_ALIVE_URL=http://ag.sprint.com/adservice/adrequest?n=keepalive`
  - `http://1weather-quark.onelouder.com/api/feed/city?citystate=`
  - `http://1weather-quark.onelouder.com/api/feed?latlon=`
  - `http://1weather.onelouder.com/afd/product.php?site=NWS&issuedby=%1$s&product=AFD&format=txt&version=1&glossary=1`
  - `http://api.virool.com/widgets/mobile_offer/SITEKEY?height=190&suid=123&width=290`
  - `http://forecast.weather.gov/MapClick.php?lat=`
  - `http://forecast.weather.gov/glossary.php?word=`
  - `market://details?id=`
  - `market://details?id=%s`
  - `market://details?id=com.google.android.gms.ads`
  - `..https://pubads.g.doubleclick.net/gampad/ads?sz=300x250&iu=/120348554/1weather-preroll&impl=s&gdfp_req=1&env=vp&output=xml_vast2&unviewed_position_start=1&url=http%3A%2F%2Faccuweather.com&description_url=http%3A%2F%2Faccuweather.com&correlato`
- Communication endpoints is a list of all potential communication endpoints Appicaptor was able to detect. This allows quick enumeration of suspicious domains, raw IP Addresses, etc..
- Communication endpoints: `.facebook.com`, `1weather-feed.onelouder.com`, `1weather-quark.onelouder.com`, `1weather.onelouder.com`, `1weatherapp.com`, `a.mologiq.net`, `accounts.google.com`, `ad6.%s.liverail.com`, `ad6.liverail.com`, `admarvel.s3.amazonaws.com`, `ads.admarvel.com`, `advrts.s3.amazonaws.com`, `ag-qa.pinsightmedia.com`, `amzn.to`, `androidads23.`

adcolony.com, api.facebook.com, api.virool.com, api.weather2020.com, app-measurement.com, ares.agoop.net, baseurl.admarvel.com, bit.ly, csi.gstatic.com, data.flurry.com, facebook.com, feeds.onelouder.com, forecast.weather.gov, geoname.onelouder.com, googleads.g.doubleclick.net, graph-video.%s, graph.%s, graph.%s.facebook.com, graph.facebook.com, log.agoop.net, login.live.com, login.yahoo.com, m.facebook.com, maps.google, nwsalert.onelouder.com, nwsalert1.onelouder.com, nwsalert2.onelouder.com, onelouder-1weather.s3.amazonaws.com, onelouder.com, play.google.com, plus.google.com, proton.flurry.com, pushpin.pinsightmedia.com, rmcdn.2mdn.net, sdk-rh.admarvel.com, sdk.ag.pinsightmedia.com, settings.crashlytics.com, ssl.google-analytics.com, stg.agoop.net, support.onelouder.com, twitter.com, video.1weatherapp.com, weather2020.com, ws.geonames.net, www.%s.facebook.com, www.facebook, www.facebook.com, www.google-analytics.com, www.google.com, www.googleapis.com, www.googletagmanager.com, www.linkedin.com, www.onelouder.com, www.paypal.com

- App communicates with servers in 6 countries.
- Communication with country: Austria, United States, Ireland, Japan, Germany, unknown
- Usage of SSL/TLS can protect the App's communication from adversaries. Tests indicate that communication is at least partly protected with SSL/TLS.
- Modifications of trust management found. Interface X509TrustManager is implemented or extended.
- Modifications of the SSL error handling detected: Class WebViewClient is extended and onReceivedSslError(...) is overwritten.
- The app loads the following HTML files via unprotected communication (http), which can be exploited by attackers to remotely change the displayed content and functionality of the app:
  - http://feeds.onelouder.com/mss/feeds
  - http://a.mologiq.net/mologiq/et
  - http://1weatherapp.com/privacy
  - http://1weather.onelouder.com/feeds/onelouder2/

- http://onelouder-1weather.s3.amazonaws.com/attribution.html
- http://geoname.onelouder.com/search
- http://1weatherapp.com/privacy#opt-out
- http://onelouder.com/1weather
- http://support.onelouder.com/forums/20218521
- http://ws.geonames.net/findNearbyPlaceName
- http://1weather.onelouder.com/afd/product.php?site=NWS&issuedby=%1$s&product=AFD&format=txt&version=1&glossary=1
- http://forecast.weather.gov/glossary.php?word=
- http://sdk-rh.admarvel.com/adhistory/upload?
- http://www.onelouder.com/terms
- http://api.virool.com/widgets/mobile_offer/SITEKEY?height=190&suid=123&width=290
- http://admarvel.s3.amazonaws.com/sdk/assets/adm_bmp/
- http://1weather-quark.onelouder.com/api/feed/city?citystate=
- http://ads.admarvel.com/fam/androidGetAd.php
- http://1weather.onelouder.com/feeds/onelouder/
- http://1weather-quark.onelouder.com/api/feed?latlon=
- http://forecast.weather.gov/MapClick.php?lat=
- http://sdk.ag.pinsightmedia.com/adgateway/adgateway
- http://a.mologiq.net/mologiq/dea
- http://api.weather2020.com/city/
- http://pushpin.pinsightmedia.com/api/1
- http://ag-qa.pinsightmedia.com/adgateway/adgateway

  - `http://geoname.onelouder.com/postalCodeSearch`
  - `http://a.mologiq.net/mologiq/deai`
  - `http://support.onelouder.com/forums/21691743`
  - `http://a.mologiq.net/mologiq/aea`

- The app loads the following JavaScript files via unprotected communication (http), which can be exploited by attackers to remotely change the displayed content and functionality of the app:
  - `http://admarvel.s3.amazonaws.com/js/admarvel_mraid_v2_complete.js`
  - `http://admarvel.s3.amazonaws.com/js/admarvel_compete_v1.1.js`
  - `http://admarvel.s3.amazonaws.com/sdk/admarvel_android_sdk_dynamic_viewport.js`
  - `http://baseurl.admarvel.com/mraid.js`
- The unprotected communication of the App via http connections can be eavesdroped or maliciously modified.
  - `http://1weather-quark.onelouder.com/api/feed/city?citystate=`
  - `http://1weather-quark.onelouder.com/api/feed?latlon=`
  - `http://1weather.onelouder.com/afd/product.php?site=NWS&issuedby=%1$s&product=AFD&format=txt&version=1&glossary=1`
  - `http://api.virool.com/widgets/mobile_offer/SITEKEY?height=190&suid=123&width=290`
  - `http://forecast.weather.gov/MapClick.php?lat=`
  - `http://forecast.weather.gov/glossary.php?word=`

Data security

- ECB mode usage identified. This mode has the disadvantage, that identical plaintext blocks are encrypted into identical ciphertext blocks. Therefore it does not hide patterns well and this mode is not recommended for use in cryptographic protocols at all.

- It is considered as a bad practice to use hard-coded cryptographic keys in the application. The following hard-coded cryptographic keys were found:
  - "0123456789012345"
  - "0123456789012346"
- The application requires the following permissions from the protection-level: NORMAL
  - ACCESS-NETWORK-STATE (Allows applications to access information about networks.)
  - VIBRATE (Allows access to the vibrator.)
  - WAKE-LOCK (Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming.)
  - ACCESS-WIFI-STATE (Allows applications to access information about Wi-Fi networks)
  - RECEIVE-BOOT-COMPLETED (Allows an application to receive the android.content.Intent ACTION-BOOT-COMPLETED that is broadcast after the system finishes booting. If you don't request this permission, you will not receive the broadcast at that time. Though holding this permission does not have any security implications, it can have a negative impact on the user experience by increasing the amount of time it takes the system to start and allowing applications to have themselves running without the user being aware of them. As such, you must explicitly declare your use of this facility to make that visible to the user.)
  - READ-EXTERNAL-STORAGE (Allows an application to read from external storage. Any app that declares the WRITE-EXTERNAL-STORAGE permission is implicitly granted this permission. Currently, this permission is not enforced and all apps still have access to read from external storage without this permission. That will change in a future release and apps will require this permission to read from external storage. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
- The application requires the following permissions from the protection-level: DANGEROUS
  - ACCESS-FINE-LOCATION (Allows an app to access precise location from location sources such as GPS, cell towers, and Wi-Fi.)

  - WRITE-EXTERNAL-STORAGE (Allows an application to write to external storage. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
  - INTERNET (Allows applications to open network sockets.)
  - ACCESS-COARSE-LOCATION (Allows an app to access approximate location derived from network location sources such as cell towers and Wi-Fi.)

- Application uses userdefined permissions. Application can access data of a foreign application which requires this permission to access data.
- Userdefined permission usage: `android.permission.ACCESS_COARSE_UPDATES`, `com.android.vending.BILLING`, `willcom.android.permission.RECEIVE_PHS_STATE`, `com.handmark.expressweather.permission.C2D_MESSAGE`, `com.google.android.c2dm.permission.RECEIVE`, `com.google.android.providers.gsf.permission.READ_GSERVICES`
- Application is propably overprivileged. Application has too much permissions. Foreign applications may be able to abuse this permission.
- The application uses a content provider for interacting with data set structures. Content providers are the standard interface that connects data in one process with code running in another process.
- Every ContentProvider defined in the application is protected by a permission. To access the interface from an external application it must request access to it. The interface is only available if an application defines these permissions.
- Indicator for JavaScript bridge to Android API usage found. JavaScript used in the application (localy stored or loaded dynamicaly) may access and execute Android SDK API calls.
- Wifi-Direct is not enabled. There is no risk for exploiting a vulnerability in the wpa-supplicant module responsible for the wlan management. (http://www.coresecurity.com/advisories/android-wifi-direct-denial-service)

Input interface security

- No indicators for file handling found. The app does not define a filter scheme to process specific files.
- The app does not use protection measures for preventing screenshots. For apps displaying sensitive data it is recommended to disable screenshots.

- The application is vulnerable to tapjacking. When the protection is not used inside an exported activity another application is able to redirect touch events to the exported activity without the users consent.

Privacy

- The Application gathers a list of installed applications. Even though some legitimate applications may use this functionality, it can be misused to send this information to third parties.
- Code obfuscation techniques were detected for the app.
- The obfuscation level UNKNOWN means that the application has the capability to dynamically load code from outside, which currently is not part of the analysis. Therefore, the obfuscation strength is not evaluated.
- Device administration features not used.
- Application reads out different unique device Ids. These unique identifiers allows to identify the device and to distinguish it from other devices. Another option for reading out these IDs allow to determine the environment. The application can determine if it is running on a real device or on a virtual/emulated device.
- Accessed unique identifier(s): `build model`, `build manufacturer`, `build product`, `build display`, `build fingerprint`, `build brand`, `IMEI/MEID`, `phone number`, `Wifi-MAC address`, `country code + mobile network code for SIM provider`, `MMC (Mobile Country Code)`, `unique Android ID`
- Indicators for usage of advertisement/tracking framework were found.
- Advertisment-/tracking frameworks found: `AdMarvel`, `Adcolony`, `Crashlytics`, `Doubleclick`, `Flurry`, `LiveRail`
- The application contains components (Activities) which are exported. This means these parts of the application are accessible or executable by other applications. An external app can write or read information/data to or from this app. Additionally components of this application can be executed. Following Activities are exported:
  - `com.handmark.expressweather.widgets.WidgetConfigure6x3Activity`
  - `com.handmark.expressweather.widgets.WidgetConfigure4x1ClockActivity`
  - `com.handmark.expressweather.widgets.WidgetConfigure4x2ClockActivity`

  - com.handmark.expressweather.SettingsDashActivity
  - com.pinsight.v8sdk.gcm.launcher.LauncherActivity
  - com.handmark.expressweather.widgets.WidgetConfigure4x2ClockSearchActivity
  - com.handmark.expressweather.widgets.WidgetConfigure2x2Activity
  - com.handmark.expressweather.widgets.WidgetConfigure1x1Activity
  - com.handmark.expressweather.widgets.WidgetConfigure4x2Activity
  - com.handmark.expressweather.widgets.WidgetConfigure4x1Activity

- In this application the allow backup option is enabled. This means the application and all application data will be included when performing a device backup. In case the application contains sensitive information these can be extracted from the backup archive or cloned onto other devices.
- Logging statements found in app. This might leak security or privacy relevant information.
- Permission READ-CONTACTS not used.
- Application reads information from different Sensors. This allows the application to track the user and/or determine the environment of the user. There was no Permission defined for camera usage, but the application contains specific API calls accessing the camera.Missing permissions despite of API calls could be an indication for missconfiguration or plugin/library code which is not used. For more detailed information application has to be reviewed manually.
- World readable/writable preference files detected which can be read/written by other applications.
  - WORLD-READABLE

Runtime Security

- The application contains a registered scheduled alarm. With such an alarm the application repeats the execution of the registered task for example every 10 hours. The following classes register scheduled tasks:

  - `jp.co.agoop.networkconnectivity.lib.service.AlarmReceiver`

- The scheduled task gets repeated in the following intervals:
  - Dynamic interval(s)
- The alarm manager has been initialized properly.
- Indicators found for dynamic code loading. The application loads executable code during runtime from a local or external source.
- Android dalvik code is loaded dynamically by the listed methods. Native code by Java Native Interface (for dynamic loading) is used.
- In the AndroidManifest.xml file the debuggable option is disabled. This prevents some attempts for debugging the application over the adb debug bridge with jdb. Depending of the used Android operating system this flag is not mandatory, in custom ROMs or rooted devices the OS may ignore this flag. On a non stock Android ROM this can still be misused for dynamic analyzes of the application or for doing runtime manipulation. This option should be disabled in released applications.
- The app is signed with a key that has a strength of 1024 bits. Google recommends to use a key with a strength of 2048 bit or more.
- Loadable libraries found:
  - `ARM 32 bit: lib/armeabi/libImmEndpointWarpJ.so`
- The Application has the permission to start automatically after booting the device. The application can execute code without userinteraction or prevention.

Test Performance

- Execution time of all tests: 0:01:35.016

3.2 AccuWeather (Android)

3.2.1 Tests

The following Table 3.3 summarizes the results of the Android app `AccuWeather` with version *4.3.7-free*.

Table 3.3: Overview of summarized test results for »AccuWeather«

App risks for enterprise usage
☒ *Implementation flaws? Yes.*

☐ *Privacy risks? No.*
☒ *Security risks? Yes.*

Blacklisted by policy

☐ *Violations of default policy? No.*

Communication security

☒ *Client communication used? Yes.*
☑ *Communication endpoints: 44 entries, see details.*
☑ *Communication with country:* `Austria`, `Netherlands`, `United States`, `Ireland`, `unknown`
☒ *SSL/TLS used? Yes.*
☑ *Domains accessed with http AND https:* `play.google.com`
☐ *Custom SSL/TLS trust manager implemented? No.*
☒ *SSL/TLS using custom error handling? Yes.*
☐ *SSL/TLS using faulty custom error handling? No.*
☐ *SSL/TLS using manual domain name verification? No.*
☒ *Unprotected HTML? Yes.*
☒ *Unprotected communication? Yes.*

Data security

☑ *Cryptographic Primitives:* `"AES/CBC/PKCS5Padding"`, `"AES/CFB/PKCS5Padding"`, `"RSA/ECB/PKCS1PADDING"`
☑ *Key derivation iteration count:* `3`
☒ *Application needs normal permissions? Yes.*
☒ *Application needs dangerous permissions? Yes.*
☒ *Application needs system/signature permissions? Yes.*
☑ *Userdefined permission usage: 6 entries, see details.*
☑ *Overprivileged permissions:* `DISABLE-KEYGUARD`, `CHANGE-CONFIGURATION`, `CHANGE-WIFI-MULTICAST-STATE`, `READ-EXTERNAL-STORAGE`
☒ *Is application overprivileged? Yes.*
☒ *Application defines content provider? Yes.*
⊟ *Content provider accessible without permission: None.*
☒ *JavaScript to SDK API bridge usage? Yes.*
☐ *WiFi-Direct enabled? No.*

Input interface security

⊟ *App can handle documents of mimeType: None.*
☐ *Screenshot protection used? No.*
☐ *Tap Jacking Protection used? No.*

Privacy

☒ *Obfuscation used? Yes.*
☑ *Obfuscation level is:* `UNKNOWN`
⊟ *Device administration policy entries: None.*
☑ *Accessed unique identifier(s): 8 entries, see details.*

☑	*Advertisment-/tracking frameworks found:* `Doubleclick`, `ScorecardResearch`, `Urban Airship`
☒	*App provides public accessible activities? Yes.*
☒	*Backup of app is allowed? Yes.*
☒	*Log Statement Enabled? Yes.*
☐	*Permission to access address book? No.*
☑	*Sensor usage:* `WIFI-Based Location`, `GPS Location`
☒	*Unprotected preference files found? Yes.*

Runtime Security

☒	*Scheduled Alarm Manager registered? Yes.*
☑	*Alarm repeating types:* `RTC`, `ELAPSED-REALTIME`, `RTC-WAKEUP`
☒	*Alarm intervals dynamically? Yes.*
☐	*Alarm Manager initialized dynamically? No.*
☒	*Dynamically loaded code at runtime? Yes.*
☑	*Dynamically loaded code at runtime type(s):* `dalvik.system.DexClassLoader(...)`, `ClassLoader.loadClass(...)`
☐	*Allow app debugging Flag? No.*
☒	*App uses outdated signature key? Yes.*
☒	*Contains native libraries: Yes.*
☑	*Executed component after Phone Reboot:* `com.accuweather.notifications.AccuNotificationBroadcastReceiver`, `com.accuweather.googlenow.GoogleNowOnBootUpReceiver`, `com.gimbal.internal.service.GimbalServiceStartStopReceiver`, `com.mobiquitynetworks.receivers.SubSystemActionsReceiver`, `org.altbeacon.beacon.startup.StartupBroadcastReceiver`

3.2.2 Details

The following sections describe details about the test results of `AccuWeather` with version *4.3.7-free*.

App risks for enterprise usage

- Reasons for category implementation flaws:
  - Possible flaw: unintended use of insecure HTTP protocol for transmissions of parameters to servers capable of HTTPS.
- Reasons for category security risks:

  - Unprotected Web Content: App loads active web content (e.g. JavaScript or HTML files) without integrity protection. This poses a risk as man-in-the-middle attackers can modify the loaded web content and change the functionality of the app.

Communication security

- Client communication detected. The application can establish a network connection to one or more specific host systems. URLs with parameters found:
  - `http://play.google.com/store/apps/details?id=com.facebook.orca`
  - `http://vortex.accuweather.com/widget/googlemaps/androidv4.1/maps.asp?lat=0&lon=0&zoomControl=false&language=`
  - `https://play.google.com/store/apps/details?id=`
  - `market://details?id=`
  - `market://details?id=com.facebook.orca`
- Communication endpoints is a list of all potential communication endpoints Appicaptor was able to detect. This allows quick enumeration of suspicious domains, raw IP Addresses, etc..
- Communication endpoints: `.facebook.com`, `accounts.google.com`, `analytics-server.gimbal.com`, `api.accuweather.com`, `api.brightcove.co.jp`, `api.brightcove.com`, `app.getsentry.com`, `b.scorecardresearch.com`, `cep.gimbal.com`, `communicate.gimbal.com`, `csi.gstatic.com`, `data.altbeacon.org`, `dev.virtualearth.net`, `devoweb.accuweather.com`, `edge.api.brightcove.com`, `facebook.com`, `googleads.g.doubleclick.net`, `graph-video.%s`, `graph.%s`, `m.accuweather.com`, `maps.googleapis.com`, `metrics.brightcove.com`, `observations.skynalysis.com`, `pagead2.googlesyndication.com`, `placebubble.gimbal.com`, `play.google.com`, `registration.gimbal.com`, `resolve.gimbal.com`, `s0.2mdn.net`, `samsungtv.accuweather.com`, `sb.scorecardresearch.com`, `sdk-configuration.gimbal.com`, `sdk-info.gimbal.com`, `sightings.gimbal.com`, `syndicate.accuweather.com`, `tilergrp.accuaws.com`, `udm.scorecardresearch.com`, `videowall.accuweather.com`, `vortex.accuweather.com`, `wvlic.brightcove.com`, `www.accuweather.com`, `www.google.com`, `www.googleapis.com`, `youtube.com`

- App communicates with servers in 5 countries.
- Usage of SSL/TLS can protect the App's communication from adversaries. Tests indicate that communication is at least partly protected with SSL/TLS.
- Mixed usage of HTTP and HTTPS: Protected and unprotected submission of parameters to the same domain. Indicates implementation flaw or weak communication protection.
- App uses the secure default SSL/TLS implementation for client communication. Error-prone modifications were not detected.
- Modifications of the SSL error handling detected: Class WebViewClient is extended and onReceivedSslError(...) is overwritten.
- The app loads the following HTML files via unprotected communication (http), which can be exploited by attackers to remotely change the displayed content and functionality of the app:
  - `http://vortex.accuweather.com/widget/googlemaps/androidv4.1/maps.asp`
  - `http://vortex.accuweather.com/widget/googlemaps/androidv4.1/maps.asp?lat=0&lon=0&zoomControl=false&language=`
  - `http://tilergrp.accuaws.com/wwa`
  - `http://samsungtv.accuweather.com/samsung/tizenwebapp/default.html`
  - `http://tilergrp.accuaws.com/csr`
  - `http://www.accuweather.com/upload-content`
  - `http://vortex.accuweather.com/widget/googlemaps/androidv4.1/maps.asp?`
  - `http://www.accuweather.com/m/EULA.aspx`
  - `http://vortex.accuweather.com/adc2010/images/google/now/padded/`
  - `http://udm.scorecardresearch.com/offline`
  - `http://s0.2mdn.net/instream/html5/native/native_sdk_v3.html`
  - `http://b.scorecardresearch.com/p2?`
  - `http://m.accuweather.com/en/privacy`
  - `http://m.accuweather.com/en/legal`

  - `http://www.accuweather.com/m/Legal/Privacy.aspx`

- The unprotected communication of the App via http connections can be eavesdroped or maliciously modified.
  - `http://play.google.com/store/apps/details?id=com.facebook.orca`
  - `http://vortex.accuweather.com/widget/googlemaps/androidv4.1/maps.asp?lat=0&lon=0&zoomControl=false&language=`

Data security

- Key derivation functions with less than 1000 interations are considered vulnerable to bruteforce attacks. Therefore, this app with 3 iterations is considered vulnerable.
- The application requires the following permissions from the protection-level: NORMAL
  - ACCESS-WIFI-STATE (Allows applications to access information about Wi-Fi networks)
  - VIBRATE (Allows access to the vibrator.)
  - ACCESS-NETWORK-STATE (Allows applications to access information about networks.)
  - WAKE-LOCK (Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming.)
  - READ-EXTERNAL-STORAGE (Allows an application to read from external storage. Any app that declares the WRITE-EXTERNAL-STORAGE permission is implicitly granted this permission. Currently, this permission is not enforced and all apps still have access to read from external storage without this permission. That will change in a future release and apps will require this permission to read from external storage. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
  - RECEIVE-BOOT-COMPLETED (Allows an application to receive the android.content.Intent ACTION-BOOT-COMPLETED that is broadcast after the system finishes booting. If you don't request this permission, you will not receive the broadcast at that time. Though holding this permission does not have any security implications, it can have a negative impact on the user experience by increasing the amount of time it takes the system to start and allowing applications to have themselves running without the user being aware of

them. As such, you must explicitly declare your use of this facility to make that visible to the user.)

- The application requires the following permissions from the protection-level: DANGEROUS
  - BLUETOOTH-ADMIN (Allows applications to discover and pair bluetooth devices.)
  - BLUETOOTH (Allows applications to connect to paired Bluetooth devices.)
  - DISABLE-KEYGUARD (Allows applications to disable the keyguard.)
  - WRITE-EXTERNAL-STORAGE (Allows an application to write to external storage. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
  - ACCESS-FINE-LOCATION (Allows an app to access precise location from location sources such as GPS, cell towers, and Wi-Fi.)
  - INTERNET (Allows applications to open network sockets.)
  - ACCESS-COARSE-LOCATION (Allows an app to access approximate location derived from network location sources such as cell towers and Wi-Fi.)
  - CHANGE-WIFI-MULTICAST-STATE (Allows applications to enter Wi-Fi Multicast mode.)
- The application requires the following permissions from the protection-level: DANGEROUS
  - CHANGE-CONFIGURATION (Allows an application to modify the current configuration, such as locale.)
- Application uses userdefined permissions. Application can access data of a foreign application which requires this permission to access data.
- Userdefined permission usage: `com.accuweather.android.permission.UA-DATA`, `com.accuweather.android.permission.RECEIVE-ADM-MESSAGE`, `com.amazon.device.messaging.permission.RECEIVE`, `com.android.vending.BILLING`, `com.accuweather.android.permission.C2D-MESSAGE`, `com.google.android.c2dm.permission.RECEIVE`
- Application is propably overprivileged. Application has too much permissions. Foreign applications may be able to abuse this permission.

- The application uses a content provider for interacting with data set structures. Content providers are the standard interface that connects data in one process with code running in another process.
- Every ContentProvider defined in the application is protected by a permission. To access the interface from an external application it must request access to it. The interface is only available if an application defines these permissions.
- Indicator for JavaScript bridge to Android API usage found. JavaScript used in the application (localy stored or loaded dynamicaly) may access and execute Android SDK API calls.
- Wifi-Direct is not enabled. There is no risk for exploiting a vulnerability in the wpa-supplicant module responsible for the wlan management. (http://www.coresecurity.com/advisories/android-wifi-direct-denial-service)

Input interface security

- No indicators for file handling found. The app does not define a filter scheme to process specific files.
- The app does not use protection measures for preventing screenshots. For apps displaying sensitive data it is recommended to disable screenshots.
- The application is vulnerable to tapjacking. When the protection is not used inside an exported activity another application is able to redirect touch events to the exported activity without the users consent.

Privacy

- Code obfuscation techniques were detected for the app.
- The obfuscation level UNKNOWN means that the application has the capability to dynamically load code from outside, which currently is not part of the analysis. Therefore, the obfuscation strength is not evaluated.
- Device administration features not used.
- Application reads out different unique device Ids. These unique identifiers allows to identify the device and to distinguish it from other devices. Another option for reading out these IDs allow to determine the environment. The application can determine if it is running on a real device or on a virtual/emulated device.
- Accessed unique identifier(s): `build model`, `build manufacturer`, `build product`, `build serial`, `build hardware`, `build display`, `build brand`, `unique Android ID`

- Indicators for usage of advertisement/tracking framework were found.
- The application contains components (Activities) which are exported. This means these parts of the application are accessible or executable by other applications. An external app can write or read information/data to or from this app. Additionally components of this application can be executed. Following Activities are exported:
  - `com.accuweather.widgets.WidgetConfigureActivityLight`
  - `com.accuweather.app.RateAppDialog`
  - `com.accuweather.widgets.WidgetConfigureActivityDark`
  - `com.accuweather.app.MainActivity`
  - `com.facebook.CustomTabActivity`
  - `com.accuweather.locations.AddressLocationSearch`
  - `com.accuweather.locations.LocationSearch`
- In this application the allow backup option is enabled. This means the application and all application data will be included when performing a device backup. In case the application contains sensitive information these can be extracted from the backup archive or cloned onto other devices.
- Logging statements found in app. This might leak security or privacy relevant information.
- Permission READ-CONTACTS not used.
- Application reads information from different sensors. This allows the application to track the user and/or determine the environment of the user.
- World readable/writable preference files detected which can be read/written by other applications.
  - WORLD-READABLE

Runtime Security

- The application contains a registered scheduled alarm. With such an alarm the application repeats the execution of the registered task for example every 10 hours. The following classes register scheduled tasks:
  - `com.accuweather.notifications.AccuNotification`

  - com.accuweather.googlenow.GoogleNowScheduler
  - com.accuweather.widgets.EdgeCocktailFeedsProvider
- The scheduled task gets repeated in the following intervals:
  - Dynamic interval(s)
  - 30 minutes
- The alarm manager has been initialized properly.
- Indicators found for dynamic code loading. The application loads executable code during runtime from a local or external source.
- Android dalvik code is loaded dynamically by the listed methods.
- In the AndroidManifest.xml file the debuggable option is disabled. This prevents some attempts for debugging the application over the adb debug bridge with jdb. Depending of the used Android operating system this flag is not mandatory, in custom ROMs or rooted devices the OS may ignore this flag. On a non stock Android ROM this can still be misused for dynamic analyzes of the application or for doing runtime manipulation. This option should be disabled in released applications.
- The app is signed with a key that has a strength of 1024 bits. Google recommends to use a key with a strength of 2048 bit or more.
- Loadable libraries found:
  - ARMv8 64 bit: lib/arm64-v8a/libcproxy.so
  - ARM 32 bit: lib/armeabi/libcproxy.so
  - ARM 32 bit: lib/armeabi-v7a/libcproxy.so
  - x86 32bit: lib/x86/libcproxy.so
- The Application has the permission to start automatically after booting the device. The application can execute code without userinteraction or prevention.

Test Performance

- Execution time of all tests: 0:01:07.167

3.3 Drops - der Regenalarm (Android)

3.3.1 Tests

The following Table 3.4 summarizes the results of the Android app `Drops – der Regenalarm` with version *3.6.7*.

Table 3.4: Overview of summarized test results for »Drops - der Regenalarm«

App risks for enterprise usage	
☐	*Implementation flaws? No.*
☒	*Privacy risks? Yes.*
☒	*Security risks? Yes.*
Blacklisted by policy	
☐	*Violations of default policy? No.*
Communication security	
☒	*Client communication used? Yes.*
☑	*Communication endpoints: 38 entries, see details.*
☑	*Communication with country: 6 entries, see details.*
☒	*SSL/TLS used? Yes.*
☒	*Custom SSL/TLS trust manager implemented? Yes.*
☐	*Faulty custom SSL/TLS trust manager implemented? No.*
☒	*SSL/TLS using custom error handling? Yes.*
☐	*SSL/TLS using faulty custom error handling? No.*
☒	*SSL/TLS using manual domain name verification? Yes.*
☒	*Unprotected HTML? Yes.*
☒	*Unprotected JavaScripts? Yes.*
☒	*Unprotected communication? Yes.*
Data security	
☑	*Cryptographic Primitives:* `"AES/CBC/PKCS5Padding", "DES/ECB/PKCS5Padding"`
☒	*Application needs normal permissions? Yes.*
☒	*Application needs dangerous permissions? Yes.*
☑	*Userdefined permission usage:* `com.android.vending.BILLING`
☑	*Overprivileged permissions:* `READ-EXTERNAL-STORAGE, RECEIVE-BOOT-COMPLETED`
☒	*Is application overprivileged? Yes.*
☒	*Application defines content provider? Yes.*
−	*Content provider accessible without permission: None.*
☒	*JavaScript to SDK API bridge usage? Yes.*
☐	*WiFi-Direct enabled? No.*
Input interface security	

⊟	*App can handle documents of mimeType: None.*
☐	*Screenshot protection used? No.*
☐	*Tap Jacking Protection used? No.*

Privacy

☒	*Installed app list accessed? Yes.*
☒	*Obfuscation used? Yes.*
☑	*Obfuscation level is:* `UNKNOWN`
⊟	*Device administration policy entries: None.*
☑	*Accessed unique identifier(s): 12 entries, see details.*
☑	*Advertisment-/tracking frameworks found:* `Branch Metrics`, `Crashlytics`, `Doubleclick`
☒	*App provides public accessible activities? Yes.*
☒	*Backup of app is allowed? Yes.*
☒	*Log Statement Enabled? Yes.*
☐	*Permission to access address book? No.*
☑	*Sensor usage:* `Camera (inactive)`, `WIFI-Based Location`, `GPS Location`, `Acceleration/Light`
☒	*Unprotected preference files found? Yes.*

Runtime Security

☒	*Scheduled Alarm Manager registered? Yes.*
☑	*Alarm repeating types:* `RTC`
☐	*Alarm intervals dynamically? No.*
☐	*Alarm Manager initialized dynamically? No.*
☒	*Dynamically loaded code at runtime? Yes.*
☑	*Dynamically loaded code at runtime type(s):* `dalvik.system.DexClassLoader(...)`, `ClassLoader.loadClass(...)`, `loadLibrary(...)`
☐	*Allow app debugging Flag? No.*
☒	*Allow autoexecute after Phone Reboot? Yes.*
☒	*App uses outdated signature key? Yes.*

3.3.2 Details

The following sections describe details about the test results of `Drops – der Regenalarm` with version *3.6.7*.

App risks for enterprise usage

- Reasons for category privacy risks:
  - App Listing: Usage of detected functionality to access list of installed apps poses a privacy risk for detected app type.
- Reasons for category security risks:

  - Unprotected Web Content: App loads active web content (e.g. JavaScript or HTML files) without integrity protection. This poses a risk as man-in-the-middle attackers can modify the loaded web content and change the functionality of the app.

Communication security

- Client communication detected. The application can establish a network connection to one or more specific host systems. URLs with parameters found:
  - `http://play.google.com/store/apps/details?id=com.facebook.orca`
  - `market://details?id=com.facebook.orca`
  - `market://details?id=com.google.android.gms.ads`
- Communication endpoints is a list of all potential communication endpoints Appicaptor was able to detect. This allows quick enumeration of suspicious domains, raw IP Addresses, etc..
- Communication endpoints: `.facebook.com`, `accounts.google.com`, `ads.wingman.do`, `api.branch.io`, `api.openweathermap.org`, `api.wingman.do`, `app.adjust.com`, `bnc.lt`, `cdn3-scripts1.widespace.com`, `csi.gstatic.com`, `e.crashlytics.com`, `engine.widespace.com`, `eu2.madsone.com`, `expand.properties`, `facebook.com`, `googleads.g.doubleclick.net`, `graph-video.%s`, `graph.%s`, `login.live.com`, `login.yahoo.com`, `maps.googleapis.com`, `orientation.properties`, `play.google.com`, `plus.google.com`, `resize.properties`, `settings.crashlytics.com`, `ssl.google-analytics.com`, `twitter.com`, `wingman.do`, `www.facebook.com`, `www.google-analytics.com`, `www.google.com`, `www.googleapis.com`, `www.googletagmanager.com`, `www.linkedin.com`, `www.moceanmobile.com`, `www.paypal.com`, `www.widespace.com`
- App communicates with servers in 6 countries.
- Communication with country: `Netherlands`, `United States`, `Ireland`, `United Kingdom`, `Germany`, `unknown`
- Usage of SSL/TLS can protect the App's communication from adversaries. Tests indicate that communication is at least partly protected with SSL/TLS.

- Modifications of trust management found. Interface X509TrustManager is implemented or extended.
- Modifications of the SSL error handling detected: Class WebViewClient is extended and onReceivedSslError(...) is overwritten.
- Correct verification of the corresponding client hostname is important for SSL/TLS security. The app changes the secure default hostname verification by the following:
  - Interface HostnameVerifier is implemented or extended.
- The app loads the following HTML files via unprotected communication (http), which can be exploited by attackers to remotely change the displayed content and functionality of the app:
  - `http://api.wingman.do/2`
  - `http://engine.widespace.com/map/engine/adnotification`
  - `http://wingman.do/schema`
  - `http://ads.wingman.do/wingman/`
  - `http://engine.widespace.com/map/provisioning`
  - `http://www.moceanmobile.com/appconversion.php`
  - `http://eu2.madsone.com/req/`
- The app loads the following JavaScript files via unprotected communication (http), which can be exploited by attackers to remotely change the displayed content and functionality of the app:
  - `http://cdn3-scripts1.widespace.com/sdk/runtime/pre-ctrl-runtime.js`
  - `http://engine.widespace.com/map/engine/dscript/mraid/2.0/nva/android/2.0.0/mraid.js`
- The unprotected communication of the App via http connections can be eavesdroped or maliciously modified.
  - `http://play.google.com/store/apps/details?id=com.facebook.orca`

Data security

- The application requires the following permissions from the protection-level: NORMAL

  - ACCESS-NETWORK-STATE (Allows applications to access information about networks.)
  - READ-EXTERNAL-STORAGE (Allows an application to read from external storage. Any app that declares the WRITE-EXTERNAL-STORAGE permission is implicitly granted this permission. Currently, this permission is not enforced and all apps still have access to read from external storage without this permission. That will change in a future release and apps will require this permission to read from external storage. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
  - WAKE-LOCK (Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming.)
  - RECEIVE-BOOT-COMPLETED (Allows an application to receive the android.content.Intent ACTION-BOOT-COMPLETED that is broadcast after the system finishes booting. If you don't request this permission, you will not receive the broadcast at that time. Though holding this permission does not have any security implications, it can have a negative impact on the user experience by increasing the amount of time it takes the system to start and allowing applications to have themselves running without the user being aware of them. As such, you must explicitly declare your use of this facility to make that visible to the user.)
  - VIBRATE (Allows access to the vibrator.)

- The application requires the following permissions from the protection-level: DANGEROUS
  - ACCESS-COARSE-LOCATION (Allows an app to access approximate location derived from network location sources such as cell towers and Wi-Fi.)
  - WRITE-EXTERNAL-STORAGE (Allows an application to write to external storage. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
  - ACCESS-FINE-LOCATION (Allows an app to access precise location from location sources such as GPS, cell towers, and Wi-Fi.)
  - INTERNET (Allows applications to open network sockets.)
- Application uses userdefined permissions. Application can access data of a foreign application which requires this permission to access data.
- Application is propably overprivileged. Application has too much permissions. Foreign applications may be able to abuse this permission.

- The application uses a content provider for interacting with data set structures. Content providers are the standard interface that connects data in one process with code running in another process.
- Every ContentProvider defined in the application is protected by a permission. To access the interface from an external application it must request access to it. The interface is only available if an application defines these permissions.
- Indicator for JavaScript bridge to Android API usage found. JavaScript used in the application (localy stored or loaded dynamicaly) may access and execute Android SDK API calls.
- Wifi-Direct is not enabled. There is no risk for exploiting a vulnerability in the wpa-supplicant module responsible for the wlan management. (http://www.coresecurity.com/advisories/android-wifi-direct-denial-service)

Input interface security

- No indicators for file handling found. The app does not define a filter scheme to process specific files.
- The app does not use protection measures for preventing screenshots. For apps displaying sensitive data it is recommended to disable screenshots.
- The application is vulnerable to tapjacking. When the protection is not used inside an exported activity another application is able to redirect touch events to the exported activity without the users consent.

Privacy

- The Application gathers a list of installed applications. Even though some legitimate applications may use this functionality, it can be misused to send this information to third parties.
- Code obfuscation techniques were detected for the app.
- The obfuscation level UNKNOWN means that the application has the capability to dynamically load code from outside, which currently is not part of the analysis. Therefore, the obfuscation strength is not evaluated.
- Device administration features not used.
- Application reads out different unique device Ids. These unique identifiers allows to identify the device and to distinguish it from other devices. Another option for reading out these IDs allow to determine the environment. The application can determine if it is running on a real device or on a virtual/emulated device.

- Accessed unique identifier(s): `build model`, `build manufacturer`, `build product`, `build serial`, `build hardware`, `build display`, `build fingerprint`, `build brand`, `IMEI/MEID`, `Wifi-MAC address`, `country code + mobile network code for SIM provider`, `unique Android ID`
- Indicators for usage of advertisement/tracking framework were found.
- The application contains components (Activities) which are exported. This means these parts of the application are accessible or executable by other applications. An external app can write or read information/data to or from this app. Additionally components of this application can be executed. Following Activities are exported:
  - `org.yoki.android.buienalarm.ui.activity.BuienAlarmLocationChooserActivity`
  - `org.yoki.android.buienalarm.ui.activity.BuienAlarmPreferenceActivity`
  - `org.yoki.android.buienalarm.ui.activity.MainActivity`
  - `org.yoki.android.buienalarm.ui.activity.SubscriptionActivity`
  - `org.yoki.android.buienalarm.ui.activity.LocationPreferencesActivity`
  - `org.yoki.android.buienalarm.widget.BuienAlarmWidgetConfigure`
- In this application the allow backup option is enabled. This means the application and all application data will be considered by doing a device backup. If an application contains sensitive information these can be cloned by backing up the data and extracted from the backup archive off device.
- Logging statements found in app. This might leak security or privacy relevant information.
- Permission READ-CONTACTS not used.
- Application reads information from different Sensors. This allows the application to track the user and/or determine the environment of the user. There was no Permission defined for camera usage, but the application contains specific API calls accessing the camera.Missing permissions despite of API calls could be an indication for missconfiguration or plugin/library code which is not used. For more detailed information application has to be reviewed manually.

- World readable/writable preference files detected which can be read/written by other applications.
  - WORLD-READABLE

Runtime Security

- The application contains a registered scheduled alarm. With such an alarm the application repeats the execution of the registered task for example every 10 hours. The following classes register scheduled tasks:
  - `org.yoki.android.buienalarm.widget.BuienAlarmWidget`
- The scheduled task gets repeated in the following intervals:
  - 5 minutes
- The alarm manager has been initialized properly.
- Indicators found for dynamic code loading. The application loads executable code during runtime from a local or external source.
- Android dalvik code is loaded dynamically by the listed methods. Native code by Java Native Interface (for dynamic loading) is used.
- In the AndroidManifest.xml file the debuggable option is disabled. This prevents some attempts for debugging the application over the adb debug bridge with jdb. Depending of the used Android operating system this flag is not mandatory, in custom ROMs or rooted devices the OS may ignore this flag. On a non stock Android ROM this can still be misused for dynamic analyzes of the application or for doing runtime manipulation. This option should be disabled in released applications.
- The Application has the permission to start automatically after booting the device. The application can execute code without userinteraction or prevention.
- The app is signed with a key that has a strength of 1024 bits. Google recommends to use a key with a strength of 2048 bit or more.

Test Performance

- Execution time of all tests: 0:01:10.655

3.4 Genaues Wetter für Deutschland (Android)

3.4.1 Tests

The following Table 3.5 summarizes the results of the Android app `Genaues Wetter für Deutschland` with version *5.6.7*.

Table 3.5: Overview of summarized test results for »Genaues Wetter für Deutschland«

App risks for enterprise usage	
☒	*Implementation flaws? Yes.*
☐	*Privacy risks? No.*
☒	*Security risks? Yes.*
Blacklisted by policy	
☐	*Violations of default policy? No.*
Communication security	
☒	*Client communication used? Yes.*
☑	*Communication endpoints: 38 entries, see details.*
☑	*Communication with country: 6 entries, see details.*
☒	*SSL/TLS used? Yes.*
☒	*Custom SSL/TLS trust manager implemented? Yes.*
☒	*Faulty custom SSL/TLS trust manager implemented? Yes.*
☒	*SSL/TLS using custom error handling? Yes.*
☒	*SSL/TLS using faulty custom error handling? Yes.*
☒	*SSL/TLS using manual domain name verification? Yes.*
☒	*Unprotected HTML? Yes.*
☒	*Unprotected communication? Yes.*
Data security	
☑	*Cryptographic Primitives:* `"RSA/ECB/PKCS1PADDING"`
☒	*Application needs normal permissions? Yes.*
☒	*Application needs dangerous permissions? Yes.*
☑	*Userdefined permission usage:* `com.amazon.device.messaging.permission.RECEIVE`, `com.weather.Weather.permission.RECEIVE-ADM-MESSAGE`, `com.google.android.c2dm.permission.RECEIVE`, `com.google.android.providers.gsf.permission.READ-GSERVICES`
☑	*Overprivileged permissions:* `GET-ACCOUNTS`, `READ-EXTERNAL-STORAGE`
☒	*Is application overprivileged? Yes.*
☒	*Application defines content provider? Yes.*
−	*Content provider accessible without permission: None.*
☒	*JavaScript to SDK API bridge usage? Yes.*
☐	*WiFi-Direct enabled? No.*

Input interface security	
⊟	*App can handle documents of mimeType: None.*
☐	*Screenshot protection used? No.*
☐	*Tap Jacking Protection used? No.*

Privacy	
☒	*Obfuscation used? Yes.*
☑	*Obfuscation level is:* `UNKNOWN`
⊟	*Device administration policy entries: None.*
☑	*Accessed unique identifier(s): 11 entries, see details.*
☑	*Advertisment-/tracking frameworks found:* `Doubleclick`, `Google Analytics`, `HockeyApp`, `ScorecardResearch`, `SessionM`
☒	*App provides public accessible activities? Yes.*
☒	*Backup of app is allowed? Yes.*
☒	*Log Statement Enabled? Yes.*
☐	*Permission to access address book? No.*
☑	*Sensor usage:* `WIFI-Based Location`, `GPS Location`

Runtime Security	
☐	*Scheduled Alarm Manager registered? No.*
☒	*Dynamically loaded code at runtime? Yes.*
☑	*Dynamically loaded code at runtime type(s):* `java.net.URLClassLoader(...)`, `ClassLoader.loadClass(...)`
☐	*Allow app debugging Flag? No.*
☒	*App uses outdated signature key? Yes.*
☑	*Executed component after Phone Reboot:* `com.weather.dal2.system.UniversalBroadcastReceiver`, `com.weather.dal2.lbs.LbsServiceController`

3.4.2 Details

The following sections describe details about the test results of `Genaues Wetter für Deutschland` with version *5.6.7*.

App risks for enterprise usage

- Reasons for category implementation flaws:
  - Possible flaw: App contains insecure code for communication protection with SSL/TLS. Common source for flawed communication protection against man-in-the-middle attacks.
- Reasons for category security risks:

- Unprotected Web Content: App loads active web content (e.g. JavaScript or HTML files) without integrity protection. This poses a risk as man-in-the-middle attackers can modify the loaded web content and change the functionality of the app.

Communication security

- Client communication detected. The application can establish a network connection to one or more specific host systems. URLs with parameters found:
  - `a.href=http://www.amazon.com/gp/feature.html?ie=UTF8&docId=1000667601`
  - `a.href=http://www.amazon.com/gp/help/customer/display.html?nodeId=468496`
  - `http://m.weather.com/safety/wxready-storm?locid=`
  - `http://triggers.weather.com/json/?resp_type=json`
  - `http://triggers.weather.com/json/?resp_type=json&zip=`
  - `https://api.mapbox.com/styles/v1/weather/cion9j5bj001pazno5y6pn5rm/static/%7BLON%7D,%7BLAT%7D,%7BZOOM%7D,0,0/%7BWIDTH%7Dx%7BHEIGHT%7D%7BRETINA%7D?access_token=%7BACCESS_TOKEN%7D`
  - `https://dsx-secure.weather.com/event/log?api=`
  - `https://dsx.weather.com/cms/assets/bigimpact?api=`
  - `https://dsx.weather.com/cms/assets/topstories?api=`
  - `https://dsx.weather.com/util/image/a/%1$s?v=%2$s&w=%3$s&h=%4$s&creativeId=%5$s`
  - `https://dsx.weather.com/util/v2/image-set/m2/%1$s,%2$s?api=`
  - `https://dsx.weather.com/util/v2/image/m2/%1$s?v=%2$s&w=%3$s&h=%4$s&api=`
  - `market://details?id=`

  - market://details?id=com.google.android.gms.ads
  - ..https://play.google.com/store/apps/details?id=com.skireport&referrer=utm_source%3DWeatherChannel%26utm_campaign%3DAffilate%2520Insta

- Communication endpoints is a list of all potential communication endpoints Appicaptor was able to detect. This allows quick enumeration of suspicious domains, raw IP Addresses, etc..
- Communication endpoints: .facebook.com, ads.sessionm.com, ads.sessionm.jp, api.facebook.com, api.mapbox.com, api.sessionm.com, api.sessionm.jp, api.tb.sessionm.com, b.scorecardresearch.com, bcp.crwdcntrl.net, dsx-secure.weather.com, dsx.weather.com, facebook.com, googleads.g.doubleclick.net, graph-video.%s, graph.%s, graph.facebook.com, image.weather.com, location.wfxtriggers.com, m.facebook.com, m.s.sessionm.com, m.weather.com, maps.googleapis.com, plus.google.com, portal.sessionm.com, portal.sessionm.jp, redcross.org, sb.scorecardresearch.com, sdk.hockeyapp.net, theweatherchannel.desk.com, triggers.weather.com, udm.scorecardresearch.com, weather.com, weather.com%s, www.google.com, www.googleapis.com, www.tourgeorgiafilm.com, www.weather.com
- App communicates with servers in 6 countries.
- Communication with country: Austria, Netherlands, United States, Ireland, Japan, unknown
- Usage of SSL/TLS can protect the App's communication from adversaries. Tests indicate that communication is at least partly protected with SSL/TLS.
- Modifications of trust management found. Interface X509TrustManager is implemented or extended.
- The SSL trust management for socket communication is modified in an insecure way. The following implementations of the X509TrustManager interface should be checked:
  - Lcom/amazon/identity/auth/device/endpoint/AbstractTokenRequest$MyHttpClient$MySSLSocketFactory$

- Modifications of the SSL error handling detected: Class WebViewClient is extended and onReceivedSslError(...) is overwritten.
- Faulty custom SSL error handling detected. The Class WebViewClient is extended and onReceiveSslError(...) is overwritten with an insecure implementation.
- Correct verification of the corresponding client hostname is important for SSL/TLS security. The app changes the secure default hostname verification by the following:
  - Interface HostnameVerifier is implemented or extended.
- The app loads the following HTML files via unprotected communication (http), which can be exploited by attackers to remotely change the displayed content and functionality of the app:
  - `http://www.weather.com/common/home/privacy.html`
  - `http://triggers.weather.com/json/?resp_type=json`
  - `http://redcross.org/mobile/`
  - `http://www.weather.com/weather/map/interactive/l/%s`
  - `http://www.weather.com/tropicalupdate`
  - `http://triggers.weather.com/json/?resp_type=json&zip=`
  - `http://m.weather.com/news/hurricane-central/main/USFL0316`
  - `http://www.weather.com/safety/severe`
  - `http://www.weather.com/common/home/legal.html`
  - `http://www.weather.com/weather/today/%s`
  - `http://image.weather.com/wireless/google/eula.html`
  - `http://m.weather.com/safety/wxready-storm?locid=`
  - `http://udm.scorecardresearch.com/offline`
  - `http://b.scorecardresearch.com/p2?`
  - `http://www.weather.com/safety/hurricanes`

- The unprotected communication of the App via http connections can be eavesdroped or maliciously modified.
  - `http://m.weather.com/safety/wxready-storm?locid=`
  - `http://triggers.weather.com/json/?resp_type=json`
  - `http://triggers.weather.com/json/?resp_type=json&zip=`

Data security

- The application requires the following permissions from the protection-level: NORMAL
  - GET-ACCOUNTS (Allows access to the list of accounts in the Accounts Service.)
  - READ-EXTERNAL-STORAGE (Allows an application to read from external storage. Any app that declares the WRITE-EXTERNAL-STORAGE permission is implicitly granted this permission. Currently, this permission is not enforced and all apps still have access to read from external storage without this permission. That will change in a future release and apps will require this permission to read from external storage. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
  - WAKE-LOCK (Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming.)
  - ACCESS-WIFI-STATE (Allows applications to access information about Wi-Fi networks)
  - ACCESS-NETWORK-STATE (Allows applications to access information about networks.)
  - VIBRATE (Allows access to the vibrator.)
  - RECEIVE-BOOT-COMPLETED (Allows an application to receive the android.content.Intent ACTION-BOOT-COMPLETED that is broadcast after the system finishes booting. If you don't request this permission, you will not receive the broadcast at that time. Though holding this permission does not have any security implications, it can have a negative impact on the user experience by increasing the amount of time it takes the system to start and allowing applications to have themselves running without the user being aware of them. As such, you must explicitly declare your use of this facility to make that visible to the user.)

- The application requires the following permissions from the protection-level: DANGEROUS
  - WRITE-EXTERNAL-STORAGE (Allows an application to write to external storage. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
  - ACCESS-FINE-LOCATION (Allows an app to access precise location from location sources such as GPS, cell towers, and Wi-Fi.)
  - READ-PHONE-STATE (Allows read only access to phone state. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
  - USE-CREDENTIALS (Allows an application to request authtokens from the AccountManager.)
  - INTERNET (Allows applications to open network sockets.)
  - ACCESS-COARSE-LOCATION (Allows an app to access approximate location derived from network location sources such as cell towers and Wi-Fi.)
- Application uses userdefined permissions. Application can access data of a foreign application which requires this permission to access data.
- Application is propably overprivileged. Application has too much permissions. Foreign applications may be able to abuse this permission.
- The application uses a content provider for interacting with data set structures. Content providers are the standard interface that connects data in one process with code running in another process.
- Every ContentProvider defined in the application is protected by a permission. To access the interface from an external application it must request access to it. The interface is only available if an application defines these permissions.
- Indicator for JavaScript bridge to Android API usage found. JavaScript used in the application (localy stored or loaded dynamicaly) may access and execute Android SDK API calls.
- Wifi-Direct is not enabled. There is no risk for exploiting a vulnerability in the wpa-supplicant module responsible for the wlan management. (http://www.coresecurity.com/advisories/android-wifi-direct-denial-service)

Input interface security

- No indicators for file handling found. The app does not define a filter scheme to process specific files.

- The app does not use protection measures for preventing screenshots. For apps displaying sensitive data it is recommended to disable screenshots.
- The application is vulnerable to tapjacking. When the protection is not used inside an exported activity another application is able to redirect touch events to the exported activity without the users consent.

Privacy

- Code obfuscation techniques were detected for the app.
- The obfuscation level UNKNOWN means that the application has the capability to dynamically load code from outside, which currently is not part of the analysis. Therefore, the obfuscation strength is not evaluated.
- Device administration features not used.
- Application reads out different unique device Ids. These unique identifiers allows to identify the device and to distinguish it from other devices. Another option for reading out these IDs allow to determine the environment. The application can determine if it is running on a real device or on a virtual/emulated device.
- Accessed unique identifier(s): `build model`, `build manufacturer`, `build product`, `build serial`, `build hardware`, `build display`, `build fingerprint`, `build brand`, `IMEI/MEID`, `MMC (Mobile Country Code)`, `unique Android ID`
- Indicators for usage of advertisement/tracking framework were found.
- The application contains components (Activities) which are exported. This means these parts of the application are accessible or executable by other applications. An external app can write or read information/data to or from this app. Additionally components of this application can be executed. Following Activities are exported:
  - `com.weather.Weather.widgets.WidgetConfigurationScreen`
  - `com.weather.Weather.ups.ui.LoginActivity`
  - `com.weather.Weather.tablet.app.TabletMainActivity`
  - `com.weather.Weather.tablet.TabletHourlyForecastActivity`
  - `com.weather.Weather.tablet.TabletDailyForecastActivity`

  - `com.weather.Weather.locations.LocationManagerActivity`
  - `com.weather.Weather.map.interactive.InteractiveMapActivity`
  - `com.weather.Weather.ups.ui.SignUpActivity`
  - `com.amazon.identity.auth.device.authorization.AuthorizationActivity`

- In this application the allow backup option is enabled. This means the application and all application data will be included when performing a device backup. In case the application contains sensitive information these can be extracted from the backup archive or cloned onto other devices.
- Logging statements found in app. This might leak security or privacy relevant information.
- Permission READ-CONTACTS not used.
- Application reads information from different sensors. This allows the application to track the user and/or determine the environment of the user.

Runtime Security

- The application does not contain a scheduled alarm.
- Indicators found for dynamic code loading. The application loads executable code during runtime from a local or external source.
- Android dalvik code is loaded dynamically by the listed methods.
- In the AndroidManifest.xml file the debuggable option is disabled. This prevents some attempts for debugging the application over the adb debug bridge with jdb. Depending of the used Android operating system this flag is not mandatory, in custom ROMs or rooted devices the OS may ignore this flag. On a non stock Android ROM this can still be misused for dynamic analyzes of the application or for doing runtime manipulation. This option should be disabled in released applications.
- The app is signed with a key that has a strength of 1024 bits. Google recommends to use a key with a strength of 2048 bit or more.
- The Application has the permission to start automatically after booting the device. The application can execute code without userinteraction or prevention.

Test Performance

- Execution time of all tests: 0:00:55.367

3.5 GO Wetter Vorhersage& Widgets (Android)

3.5.1 Tests

The following Table 3.6 summarizes the results of the Android app `GO Wetter Vorhersage& Widgets` with version *5.733*.

Table 3.6: Overview of summarized test results for »GO Wetter Vorhersage& Widgets«

App risks for enterprise usage	
☒	*Implementation flaws? Yes.*
☒	*Privacy risks? Yes.*
☒	*Security risks? Yes.*
Blacklisted by policy	
☒	*Violations of default policy? Yes.*
Communication security	
☒	*Client communication used? Yes.*
☑	*Communication endpoints: 68 entries, see details.*
☑	*Communication with country: 6 entries, see details.*
☒	*SSL/TLS used? Yes.*
☑	*Domains accessed with http AND https:* `play.google.com`
☒	*Custom SSL/TLS trust manager implemented? Yes.*
☒	*Faulty custom SSL/TLS trust manager implemented? Yes.*
☒	*SSL/TLS using custom error handling? Yes.*
☐	*SSL/TLS using faulty custom error handling? No.*
☒	*SSL/TLS using manual domain name verification? Yes.*
☒	*Unprotected HTML? Yes.*
☒	*Unprotected communication? Yes.*
Data security	
☑	*Cryptographic Primitives:* `"AES/CBC/PKCS5Padding"`, `"AES/ECB/PKCS7Padding"`, `"DES/ECB/PKCS7Padding"`, `"DESede"`
☒	*Cryptographic keys found? Yes.*
☒	*Application needs normal permissions? Yes.*
☒	*Application needs dangerous permissions? Yes.*
☒	*Application needs system/signature permissions? Yes.*
☑	*Userdefined permission usage:* `com.google.android.c2dm.permission.RECEIVE`, `com.google.android.providers.gsf.permission.READ-GSERVICES`, `com.gau.go.launcherex.gowidget.weatherwidget.permission.C2D-MESSAGE`, `com.gau.go.launcherex.gowidget.weatherwidget.permission.SERVICE`, `com.android.vending.BILLING`

☑ *Overprivileged permissions:* `SYSTEM-ALERT-WINDOW`, `MOUNT-UNMOUNT-FILESYSTEMS`, `READ-EXTERNAL-STORAGE`, `ACCESS-MOCK-LOCATION`
☒ *Is application overprivileged? Yes.*
☒ *Application defines content provider? Yes.*
− *Content provider accessible without permission: None.*
☒ *JavaScript to SDK API bridge usage? Yes.*
☒ i *JavaScript to SDK API bridge vulnerability? Yes. (see details)*
☐ *WiFi-Direct enabled? No.*

Input interface security

− *App can handle documents of mimeType: None.*
☐ *Screenshot protection used? No.*
☐ *Tap Jacking Protection used? No.*

Privacy

☒ *Installed app list accessed? Yes.*
☒ *Obfuscation used? Yes.*
☑ *Obfuscation level is:* `HIGH`
− *Device administration policy entries: None.*
☑ *Accessed unique identifier(s): 11 entries, see details.*
☑ *Advertisment-/tracking frameworks found:* `Doubleclick`, `Google Analytics`, `LiveRail`
☒ *App provides public accessible activities? Yes.*
☒ *Backup of app is allowed? Yes.*
☒ *Log Statement Enabled? Yes.*
☐ *Permission to access address book? No.*
☑ *Sensor usage:* `WIFI-Based Location`, `GPS Location`
☒ *Unprotected preference files found? Yes.*

Runtime Security

☒ *Scheduled Alarm Manager registered? Yes.*
☑ *Alarm repeating types:* `RTC-WAKEUP`
☐ *Alarm intervals dynamically? No.*
☐ *Alarm Manager initialized dynamically? No.*
☒ *Dynamically loaded code at runtime? Yes.*
☑ *Dynamically loaded code at runtime type(s):* `dalvik.system.DexClassLoader(...)`, `ClassLoader.loadClass(...)`, `loadLibrary(...)`
☐ *Allow app debugging Flag? No.*
☒ *App uses outdated signature key? Yes.*
☒ *Contains native libraries: Yes.*
☑ *Executed component after Phone Reboot: 6 entries, see details.*

3.5.2 Details

The following sections describe details about the test results of `GO Wetter Vorhersage& Widgets` with version *5.733*.

App risks for enterprise usage

- Reasons for category implementation flaws:
  - Possible flaw: App contains insecure code for communication protection with SSL/TLS. Common source for flawed communication protection against man-in-the-middle attacks.
  - Possible flaw: unintended use of insecure HTTP protocol for transmissions of parameters to servers capable of HTTPS.
  - Possible flaw: An application calling Android API methods by JavaScript and defining targetSdk version less than 17 could be vulnerable to remote code injection.
- Reasons for category privacy risks:
  - App Listing: Usage of detected functionality to access list of installed apps poses a privacy risk for detected app type.
- Reasons for category security risks:
  - Unprotected Web Content: App loads active web content (e.g. JavaScript or HTML files) without integrity protection. This poses a risk as man-in-the-middle attackers can modify the loaded web content and change the functionality of the app.
  - Crypto: Embedded static encryption key found, which can be extracted by attackers to revert the encryption or fake the signature of the content it is used for.

Blacklisted by policy

- Reasons for category violations of default policy:
  - Estimated overall app risk for the enterprise exceeds the security policy threshold due to detected risks and flaws exploitable by skilled attackers without the existence of additional supporting factors.

Communication security

- Client communication detected. The application can establish a network connection to one or more specific host systems. URLs with parameters found:

- http://61.145.124.212:8083/GOClientData/DR?ptl=10&is_zip=1
- http://abtest.goforandroid.com/abtestcenter/ab?gzip=0&sid=%s&cid=%d&cversion=%d&local=%s&utm_source=%s&entrance=%d&cdays=%d&isupgrade=%d&aid=%s&sdk_stat=%d
- http://csr.goforandroid.com/consume_record/common?funid=1&rd=
- http://gocurrency.goforandroid.com/gocurrency/common?funid=2&rd=
- http://gostat.3g.cn/GOClientData/DR?ptl=10&is_zip=1
- http://gotest.3g.net.cn/newstore/common?funid=20&rd=
- http://goupdate.3g.cn/GOClientData/DR?ptl=10&is_zip=1
- http://market.android.com/support/bin/answer.py?answer=1050566&hl=%lang%&dl=%region%
- http://newstoredata.goforandroid.com/newstore/common?funid=20&rd=
- http://newstoredata.goforandroid.com/newstore/usertype?buychannel=
- http://play.google.com/store/apps/details?id=
- http://spreadsheets.google.com/formResponse?formkey=
- http://wireless.mapbar.com/reverse/reverseGeocoding.json?q=
- http://www.amazon.com/gp/mas/dl/android?p=com.gtp.nextlauncher
- http://www.amazon.com/gp/mas/dl/android?p=com.gtp.nextlauncher.trial
- http://www.facebook.com/pages/GO-Weather-EX/488274257857852?ref=hl
- http://www.isvd-jhn.com/integ/sungy.html?w=

- https://play.google.com/store/apps/details?id=
- https://play.google.com/store/apps/details?id=com.gau.go.launcherex&referrer=utm_source%3DGOWeatherEX_GOwidgetRecommend%26utm_medium%3DHyperlink%26utm_campaign%3DGOWeatherEX_GOwidgetRecommend
- https://play.google.com/store/apps/details?id=com.gau.go.launcherex.gowidget.weatherwidget&referrer=utm_source%3Dthemeupdate%26utm_medium%3DHyperlink%26utm_campaign%3Dthemes
- market://details?id=
- market://details?id=%s
- market://details?id=com.gau.go.launcherex&referrer=utm_source%3DGOWeatherEX_GOwidgetRecommend%26utm_medium%3DHyperlink%26utm_campaign%3DGOWeatherEX_GOwidgetRecommend
- market://details?id=com.gau.go.launcherex&referrer=utm_source%3DGOweatherFullScreen%26utm_medium%3Dbanner%26utm_campaign%3DGOAPP
- market://details?id=com.gau.go.launcherex&referrer=utm_source%3DGOweatherGIF%26utm_medium%3Dbanner%26utm_campaign%3DGOAPP
- market://details?id=com.gau.go.launcherex&referrer=utm_source%3Dkeyboard_store%26utm_medium%3DHyperlink%26utm_campaign%3Dgolauncher
- market://details?id=com.gau.go.launcherex&referrer=utm_source%3Dsms_store%26utm_medium%3DHyperlink%26utm_campaign%3Dgolauncher
- market://details?id=com.gau.go.launcherex.gowidget.weatherwidget&referrer=utm_source%3Dkeyboard_store%26utm_medium%3DHyperlink%26utm_campaign%3Dthemestore
- market://details?id=com.gau.go.launcherex.gowidget.weatherwidget&referrer=utm_source%

3Dsms_store%26utm_medium%3DHyperlink%26utm_campaign%3Dthemestore

- market://details?id=com.gau.go.launcherex.gowidget.weatherwidget&referrer=utm_source%3Dthemeupdate%26utm_medium%3DHyperlink%26utm_campaign%3Dthemes
- market://details?id=com.gau.go.launcherex.zh
- market://details?id=com.google.android.gms.ads
- market://details?id=com.gtp.nextlauncher&referrer=utm_source%3DGOWeather%26utm_medium%3DHyperlink%26utm_campaign%3DNextWeather
- market://details?id=com.gtp.nextlauncher.trial&referrer=utm_source%3DGOWeather%26utm_medium%3DHyperlink%26utm_campaign%3DNextWeather
- market://details?id=com.jb.gokeyboard&referrer=utm_source%3DGOKEYBOARD%26utm_medium%3Dhyperlink%26utm_campaign%3DNewStoreSMS
- market://details?id=com.jb.gosms&referrer=utm_source%3DGOSMS%26utm_medium%3Dhyperlink%26utm_campaign%3DNewStoreKeybo
- market://details?id=com.jiubang.goscreenlock&referrer=utm_source%3DGOKeyboardStore%26utm_medium%3Dbanner%26utm_campaign%3DGOthemeStore
- market://details?id=com.jiubang.goscreenlock&referrer=utm_source%3DGOSMSStore%26utm_medium%3Dbanner%26utm_campaign%3DGOthemeStore
- market://details?id=com.kittyplay.ex&referrer=utm_source%3Dweather%26utm_medium%3DHyperlink%26utm_campaign%3Dgetmorethemes
- market://search?q=
- market://search?q=pname:

- Communication endpoints is a list of all potential communication endpoints Appicaptor was able to detect. This allows quick enumeration of suspicious domains, raw IP Addresses, etc..
- Communication endpoints: `3g.cn`, `abtest.goforandroid.com`, `accounts.google.com`, `activatecode.3g.cn`, `ad6.%s.liverail.com`, `ad6.liverail.com`, `adpush.goforandroid.com`, `adviap.goforandroid.com`, `advonline.goforandroid.com`, `advs2sonline.goforandroid.com`, `advsearch.goforandroid.com`, `api.appsflyer.com`, `api.goforandroid.com`, `crowdin.net`, `csi.gstatic.com`, `csr.goforandroid.com`, `events.appsflyer.com`, `goaccount.goforandroid.com`, `goadv.3g.cn`, `goappcenter.3g.cn`, `goappcenter.goforandroid.com`, `goappcenter.goforandroid.mobi`, `goappdl.goforandroid.com`, `gocurrency.goforandroid.com`, `godfs.3g.cn`, `goload.wecloud.io`, `googleads.g.doubleclick.net`, `gostat.3g.cn`, `gostore.3g.cn`, `gotest.3g.net.cn`, `goupdate.3g.cn`, `goweatherex.3g.cn`, `goweatherexmg.3g.cn`, `gows.goforandroid.com`, `graph.%s.facebook.com`, `graph.facebook.com`, `gwm.3g.cn`, `imupdate.3g.cn`, `integralwall.goforandroid.com`, `lh3.ggpht.com`, `lh3.googleusercontent.com`, `lh5.ggpht.com`, `lh6.ggpht.com`, `login.live.com`, `login.yahoo.com`, `m.facebook.com`, `market.android.com`, `newstoredata.goforandroid.com`, `play.google.com`, `plus.google.com`, `register.appsflyer.com`, `service.goforandroid.com`, `spreadsheets.google.com`, `stats.appsflyer.com`, `t.appsflyer.com`, `twitter.com`, `version.api.goforandroid.com`, `wireless.mapbar.com`, `www.%s.facebook.com`, `www.amazon.com`, `www.facebook.com`, `www.google-analytics.com`, `www.google.com`, `www.googleapis.com`, `www.isvd-jhn.com`, `www.linkedin.com`, `www.paypal.com`, `www.retailmenot.com`
- App communicates with servers in 6 countries.
- Communication with country: `Netherlands`, `Hong Kong`, `United States`, `China`, `Ireland`, `unknown`
- Usage of SSL/TLS can protect the App's communication from adversaries. Tests indicate that communication is at least partly protected with SSL/TLS.
- Mixed usage of HTTP and HTTPS: Protected and unprotected submission of parameters to the same domain. Indicates implementation flaw or weak communication protection.

- Modifications of trust management found. Interface X509TrustManager is implemented or extended.
- The SSL trust management for socket communication is modified in an insecure way. The following implementations of the X509TrustManager interface should be checked:
  - `Lcom/jiubang/core/util/NaiveTrustManager.`
  - `Lcom/jiubang/lock/a/e.`
- Modifications of the SSL error handling detected: Class WebViewClient is extended and onReceivedSslError(...) is overwritten.
- Correct verification of the corresponding client hostname is important for SSL/TLS security. The app changes the secure default hostname verification by the following:
  - Class AllowAllHostnameVerifier is used or extended.
- The app loads the following HTML files via unprotected communication (http), which can be exploited by attackers to remotely change the displayed content and functionality of the app:
  - `http://www.isvd-jhn.com/integ/sungy.html?w=`
  - `http://gocurrency.goforandroid.com/gocurrency/common?funid=2&rd=`
  - `http://goaccount.goforandroid.com/api/v2/register`
  - `http://integralwall.goforandroid.com/IntegralWall/accountOper`
  - `http://advonline.goforandroid.com/adv_online/onlineadv`
  - `http://adviap.goforandroid.com/adv_iap/integralwall`
  - `http://www.facebook.com/pages/GO-Weather-EX/488274257857852?ref=hl`
  - `http://gwm.3g.cn:8099/goweatherexMeteor/satellite/v2/image`
  - `http://gotest.3g.net.cn/newstore/common?funid=20&rd=`
  - `http://newstoredata.goforandroid.com/newstore/`

- http://advsearch.goforandroid.com/adv_search/search
- http://newstoredata.goforandroid.com/newstore/usertype?buychannel=
- http://goload.wecloud.io/goload
- http://spreadsheets.google.com/formResponse?formkey=
- http://goweatherexmg.3g.cn/goweatherexms/feedBack/gps
- http://adviap.goforandroid.com/adv_iap/userTag
- http://newstoredata.goforandroid.com/newstore/common?funid=20&rd=
- http://goweatherex.3g.cn/goweatherex/weather/getWeather
- http://adviap.goforandroid.com/adv_iap/smartload_install
- http://service.goforandroid.com/goweather/service_en.html
- http://crowdin.net/project/goweather/invite
- http://goupdate.3g.cn/GOClientData/DC
- http://play.google.com/store/apps/details
- http://advs2sonline.goforandroid.com/s2sadv
- http://gostore.3g.cn/gostore/entrance
- http://service.goforandroid.com/goweather/service_zh.html
- http://abtest.goforandroid.com/abtestcenter/ab
- http://gotest.3g.net.cn/newstore/
- http://goweatherex.3g.cn/goweatherexUninstall/weather/getUninstall
- http://goupdate.3g.cn/GOClientData/DR
- http://gostat.3g.cn/GOClientData/DR?ptl=10&is_zip=1

  - http://play.google.com/store/apps/details?id=
  - http://abtest.goforandroid.com/abtestcenter/ab?gzip=0&sid=%s&cid=%d&cversion=%d&local=%s&utm_source=%s&entrance=%d&cdays=%d&isupgrade=%d&aid=%s&sdk_stat=%d
  - http://adviap.goforandroid.com/adv_iap/smartload
  - http://www.retailmenot.com/ajax/sendCouponEmail.php
  - http://adpush.goforandroid.com/abtestcenter/
  - http://imupdate.3g.cn:8888/versions/check?
  - http://gows.goforandroid.com/goweatherexSns/coupon/couponlist
  - http://csr.goforandroid.com/consume_record/common?funid=1&rd=
  - http://goupdate.3g.cn/GOClientData/DR?ptl=10&is_zip=1
  - http://gwm.3g.cn:8099/goweatherexMeteor/satellite/image
  - http://goweatherex.3g.cn/goweatherex/city/gps
  - http://goadv.3g.cn/GoAdCenter/common
  - http://goweatherexmg.3g.cn/goweatherexms/feedBack/weather

- The unprotected communication of the App via http connections can be eavesdroped or maliciously modified.
  - http://abtest.goforandroid.com/abtestcenter/ab?gzip=0&sid=%s&cid=%d&cversion=%d&local=%s&utm_source=%s&entrance=%d&cdays=%d&isupgrade=%d&aid=%s&sdk_stat=%d
  - http://csr.goforandroid.com/consume_record/common?funid=1&rd=
  - http://gocurrency.goforandroid.com/gocurrency/common?funid=2&rd=
  - http://gostat.3g.cn/GOClientData/DR?ptl=10&is_zip=1

- http://gotest.3g.net.cn/newstore/common?funid=20&rd=
- http://goupdate.3g.cn/GOClientData/DR?ptl=10&is_zip=1
- http://market.android.com/support/bin/answer.py?answer=1050566&hl=%lang%&dl=%region%
- http://newstoredata.goforandroid.com/newstore/common?funid=20&rd=
- http://newstoredata.goforandroid.com/newstore/usertype?buychannel=
- http://play.google.com/store/apps/details?id=
- http://spreadsheets.google.com/formResponse?formkey=
- http://wireless.mapbar.com/reverse/reverseGeocoding.json?q=
- http://www.amazon.com/gp/mas/dl/android?p=com.gtp.nextlauncher
- http://www.amazon.com/gp/mas/dl/android?p=com.gtp.nextlauncher.trial
- http://www.facebook.com/pages/GO-Weather-EX/488274257857852?ref=hl
- http://www.isvd-jhn.com/integ/sungy.html?w=

Data security

- ECB mode usage identified. This mode has the disadvantage, that identical plaintext blocks are encrypted into identical ciphertext blocks. Therefore it does not hide patterns well and this mode is not recommended for use in cryptographic protocols at all.
- It is considered as a bad practice to use hard-coded cryptographic keys in the application. The following hard-coded cryptographic keys were found:
  - "NaubrwWEGiJEQqRxx7aXntbGOf4YiRmW0WY9043rcqRhJreE4sReMC1OFRaeI7T
  - "guangzhou-huizhiwccpcomm"
- The application requires the following permissions from the protection-level: NORMAL

  - RECEIVE-BOOT-COMPLETED (Allows an application to receive the android.content.Intent ACTION-BOOT-COMPLETED that is broadcast after the system finishes booting. If you don't request this permission, you will not receive the broadcast at that time. Though holding this permission does not have any security implications, it can have a negative impact on the user experience by increasing the amount of time it takes the system to start and allowing applications to have themselves running without the user being aware of them. As such, you must explicitly declare your use of this facility to make that visible to the user.)
  - ACCESS-WIFI-STATE (Allows applications to access information about Wi-Fi networks)
  - READ-EXTERNAL-STORAGE (Allows an application to read from external storage. Any app that declares the WRITE-EXTERNAL-STORAGE permission is implicitly granted this permission. Currently, this permission is not enforced and all apps still have access to read from external storage without this permission. That will change in a future release and apps will require this permission to read from external storage. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
  - WRITE-SETTINGS (Allows an application to read or write the system settings.)
  - GET-ACCOUNTS (Allows access to the list of accounts in the Accounts Service.)
  - ACCESS-NETWORK-STATE (Allows applications to access information about networks.)
  - SET-WALLPAPER (Allows applications to set the wallpaper.)
  - BROADCAST-STICKY (Allows an application to broadcast sticky intents. These are broadcasts whose data is held by the system after being finished, so that clients can quickly retrieve that data without havingto wait for the next broadcast.)
  - WAKE-LOCK (Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming.)
  - VIBRATE (Allows access to the vibrator.)

- The application requires the following permissions from the protectionlevel: DANGEROUS
  - ACCESS-MOCK-LOCATION (Allows an application to create mock location providers for testing.)

  - DISABLE-KEYGUARD (Allows applications to disable the keyguard.)
  - CHANGE-WIFI-STATE (Allows applications to change Wi-Fi connectivity state.)
  - WRITE-EXTERNAL-STORAGE (Allows an application to write to external storage. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
  - READ-PHONE-STATE (Allows read only access to phone state. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
  - ACCESS-COARSE-LOCATION (Allows an app to access approximate location derived from network location sources such as cell towers and Wi-Fi.)
  - ACCESS-FINE-LOCATION (Allows an app to access precise location from location sources such as GPS, cell towers, and Wi-Fi.)
  - GET-TASKS (Allows an application to get information about the currently or recently running tasks.)
  - SYSTEM-ALERT-WINDOW (Allows an application to open windows using the type android.view.WindowManager.LayoutParams TYPE-SYSTEM-ALERT, shown on top of all other applications. Very few applications should use this permission. these windows are intended for system-level interaction with the user.)
  - INTERNET (Allows applications to open network sockets.)

- The application requires the following permissions from the protection-level: DANGEROUS
  - MOUNT-UNMOUNT-FILESYSTEMS (Allows mounting and unmounting file systems for removable storage. Not for use by third-party applications.)
- Application uses userdefined permissions. Application can access data of a foreign application which requires this permission to access data.
- Application is propably overprivileged. Application has too much permissions. Foreign applications may be able to abuse this permission.
- The application uses a content provider for interacting with data set structures. Content providers are the standard interface that connects data in one process with code running in another process.
- Every ContentProvider defined in the application is protected by a permission. To access the interface from an external application it must request access to it. The interface is only available if an application defines these permissions.

- Indicator for JavaScript bridge to Android API usage found. JavaScript used in the application (localy stored or loaded dynamicaly) may access and execute Android SDK API calls.
- JavaScript to SDK API bridge vulnerability found: TargetSdk definition in the AndroidManifest.xml file is version: 11 . An application calling Android API methods by JavaScript and defining targetSdk version less than 17 could be vulnerable to remote code injection. For remote code injection the application has to load JavaScript or HTML code containing JavaScript code from a (generic) url.
- Wifi-Direct is not enabled. There is no risk for exploiting a vulnerability in the wpa-supplicant module responsible for the wlan management. (http://www.coresecurity.com/advisories/android-wifi-direct-denial-service)

Input interface security

- No indicators for file handling found. The app does not define a filter scheme to process specific files.
- The app does not use protection measures for preventing screenshots. For apps displaying sensitive data it is recommended to disable screenshots.
- The application is vulnerable to tapjacking. When the protection is not used inside an exported activity another application is able to redirect touch events to the exported activity without the users consent.

Privacy

- The Application gathers a list of installed applications. Even though some legitimate applications may use this functionality, it can be misused to send this information to third parties.
- Code obfuscation techniques were detected for the app.
- Obfuscation levels are rated as LOW, MEDIUM, ABOVE MEDIUM, HIGH or UNKNOWN. The detected obfuscation level of HIGH provides sophisticated protection against manual analysis which requires a high effort and deep knowledge to reverse the functionality of the app.
- Device administration features not used.
- Application reads out different unique device Ids. These unique identifiers allows to identify the device and to distinguish it from other devices. Another option for reading out these IDs allow to determine the environment. The application can determine if it is running on a real device or on a virtual/emulated device.

- Accessed unique identifier(s): `build model`, `build manufacturer`, `build product`, `build display`, `build fingerprint`, `build brand`, `IMEI/MEID`, `SIM card serial`, `subscriber ID (IMSI)`, `country code + mobile network code for SIM provider`, `unique Android ID`
- Indicators for usage of advertisement/tracking framework were found.
- The application contains components (Activities) which are exported. This means these parts of the application are accessible or executable by other applications. An external app can write or read information/data to or from this app. Additionally components of this application can be executed. Following Activities are exported:
  - `com.gau.go.launcherex.gowidget.weather.view.Setting42Activity`
  - `com.gau.go.launcherex.goweather.goplay.ThemeDetailActivity`
  - `com.gtp.go.weather.coupon.view.CouponsActivity`
  - `com.jiubang.commerce.tokencoin.integralwall.main.IntegralwallActivity`
  - `com.gau.go.launcherex.gowidget.weather.view.AppListActivity`
  - `com.go.weatherex.themeconfig.AppWidgetThemeConfigHomeActivity`
  - `com.jiubang.commerce.chargelocker.ChargeBatteryActivity`
  - `com.gau.go.launcherex.gowidget.weather.view.Setting41Activity`
  - `com.jiubang.core.util.CrashReportDialog`
  - `com.go.weatherex.themeconfig.GoWidget41ThemeConfigHomeActivity`
  - `com.jiubang.commerce.dynamicloadlib.PluginActivity`
  - `com.go.weatherex.themeconfig.GoWidgetDays41ThemeConfigHomeActivity`
  - `com.go.weatherex.managegood.view.ManageGoodPaymentActivity`

  - com.gtp.nextlauncher.widget.nextpanel.MainActivity
  - com.gau.go.launcherex.gowidget.weather.view.WeatherDetailActivity
  - com.gau.go.launcherex.gowidget.billing.BillingTabFragmentActivity
  - com.gau.go.launcherex.gowidget.weather.view.Setting21Activity
  - com.gau.go.launcherex.gowidget.weather.view.LanguageSetting
  - com.gtp.go.weather.billing.view.PayActivity
  - com.gau.go.launcherex.gowidget.weather.view.ThemeSettingActivity
  - com.gau.go.launcherex.gowidget.messagecenter.view.HtmlMsgDialogActivity
  - com.gtp.go.weather.coupon.view.CouponCollectActivity
  - com.go.weatherex.themeconfig.GoWidget21ThemeConfigHomeActivity
  - com.go.weatherex.themeconfig.GoWidgetDays42ThemeConfigHomeActivity
  - com.go.weatherex.themeconfig.GoWidget42ThemeConfigHomeActivity
  - com.go.weatherex.setting.LiveWallpaperSettingsActivity
  - com.gau.go.launcherex.gowidget.framework.GLWidgetActivity
  - com.gau.go.launcherex.gowidget.framework.GLGoWidgetActivity
  - com.gau.go.launcherex.gowidget.weather.globaltheme.view.MyCouponsActivity

- In this application the allow backup option is enabled. This means the application and all application data will be included when performing a device backup. In case the application contains sensitive information these can be extracted from the backup archive or cloned onto other devices.

- Logging statements found in app. This might leak security or privacy relevant information.
- Permission READ-CONTACTS not used.
- Application reads information from different sensors. This allows the application to track the user and/or determine the environment of the user.
- World readable/writable preference files detected which can be read/written by other applications.
  - WORLD-WRITEABLE
  - WORLD-READABLE

Runtime Security

- The application contains a registered scheduled alarm. With such an alarm the application repeats the execution of the registered task for example every 10 hours. The following classes register scheduled tasks:
  - `com.jiubang.commerce.daemon.a.a`
  - `com.gau.go.launcherex.gowidget.gcm.b`
  - `com.jiubang.dailyremmend.d`
  - `com.gau.go.launcherex.gowidget.weather.b.n`
- The scheduled task gets repeated in the following intervals:
  - 24 hours
  - 0 seconds
  - 5 minutes
- The alarm manager has been initialized properly.
- Indicators found for dynamic code loading. The application loads executable code during runtime from a local or external source.
- Android dalvik code is loaded dynamically by the listed methods. Native code by Java Native Interface (for dynamic loading) is used.
- In the AndroidManifest.xml file the debuggable option is disabled. This prevents some attempts for debugging the application over the adb debug bridge with jdb. Depending of the used Android operating system this flag is not mandatory, in custom ROMs or rooted devices the OS may ignore this flag. On a non stock Android ROM this can still be misused for dynamic analyzes of the application or for doing runtime manipulation. This option should be disabled in released applications.

- The app is signed with a key that has a strength of 1024 bits. Google recommends to use a key with a strength of 2048 bit or more.
- Loadable libraries found:
  - `ARMv8 64 bit: assets/arm64-v8a/godaemon`
  - `ARM 32 bit: assets/armeabi-v7a/godaemon`
  - `ARM 32 bit: assets/armeabi/godaemon`
  - `x86 32bit: assets/x86/godaemon`
  - `x86 64bit: assets/x86_64/godaemon`
  - `ARMv8 64 bit: lib/arm64-v8a/libdaemon_api21.so`
  - `ARM 32 bit: lib/armeabi-v7a/libdaemon_api21.so`
  - `ARM 32 bit: lib/armeabi/libdaemon_api21.so`
  - `x86 32bit: lib/x86/libdaemon_api21.so`
  - `x86 64bit: lib/x86_64/libdaemon_api21.so`
- The Application has the permission to start automatically after booting the device. The application can execute code without userinteraction or prevention.
- Executed component after Phone Reboot: `com.gau.go.launcherex.gowidget.framework.SystemBootReceiver`, `io.wecloud.message.PushServiceReceiver`, `com.jiubang.commerce.receiver.BootBroadcastReceiver`, `com.jiubang.lock.keyguard.KeyguardBootReceiver`, `com.jiubang.commerce.daemon.BootCompleteReceiver`, `com.commerce.notification.main.core.autostart.AutoStartBroadcastReceiver`

Test Performance

- Execution time of all tests: 0:01:30.298

3.6 RainToday . HD Regenradar (Android)

3.6.1 Tests

The following Table 3.7 summarizes the results of the Android app `RainToday . HD Regenradar` with version *1.5.1*.

Table 3.7: Overview of summarized test results for »RainToday . HD Regenradar«

App risks for enterprise usage	
☐	*Implementation flaws? No.*
☒	*Privacy risks? Yes.*
☒	*Security risks? Yes.*
Blacklisted by policy	
☐	*Violations of default policy? No.*
Communication security	
☒	*Client communication used? Yes.*
☑	*Communication endpoints: 26 entries, see details.*
☑	*Communication with country:* `Netherlands`, `United States`, `Ireland`, `United Kingdom`, `Germany`
☒	*SSL/TLS used? Yes.*
☒	*Custom SSL/TLS trust manager implemented? Yes.*
☐	*Faulty custom SSL/TLS trust manager implemented? No.*
☒	*SSL/TLS using custom error handling? Yes.*
☐	*SSL/TLS using faulty custom error handling? No.*
☐	*SSL/TLS using manual domain name verification? No.*
☒	*Unprotected HTML? Yes.*
☒	*Unprotected communication? Yes.*
Data security	
☑	*Cryptographic Primitives:* `"AES/CBC/PKCS5Padding"`
☒	*Application needs normal permissions? Yes.*
☒	*Application needs dangerous permissions? Yes.*
☑	*Userdefined permission usage: 6 entries, see details.*
☑	*Overprivileged permissions:* `GET_ACCOUNTS`, `READ_EXTERNAL_STORAGE`
☒	*Is application overprivileged? Yes.*
☒	*JavaScript to SDK API bridge usage? Yes.*
☐	*WiFi-Direct enabled? No.*
Input interface security	
⊟	*App can handle documents of mimeType: None.*
☐	*Screenshot protection used? No.*
☐	*Tap Jacking Protection used? No.*
Privacy	
☒	*Installed app list accessed? Yes.*
☒	*Obfuscation used? Yes.*
☑	*Obfuscation level is:* `HIGH`
⊟	*Device administration policy entries: None.*
☑	*Accessed unique identifier(s): 11 entries, see details.*
☑	*Advertisment-/tracking frameworks found:* `Crashlytics`, `Doubleclick`

☒	*App provides public accessible activities? Yes.*
☒	*Backup of app is allowed? Yes.*
☒	*Log Statement Enabled? Yes.*
☐	*Permission to access address book? No.*
☑	*Sensor usage:* `WIFI-Based Location`, `GPS Location`, `Acceleration/Light`
☒	*Unprotected preference files found? Yes.*

Runtime Security

☐	*Scheduled Alarm Manager registered? No.*
☒	*Dynamically loaded code at runtime? Yes.*
☑	*Dynamically loaded code at runtime type(s):* `dalvik.system.DexClassLoader(...)`, `dalvik.system.PathClassLoader(...)`, `ClassLoader.loadClass(...)`, `loadLibrary(...)`
☐	*Allow app debugging Flag? No.*
☒	*App uses outdated signature key? Yes.*
☒	*Contains native libraries: Yes.*
☑	*Executed component after Phone Reboot:* `com.mg.raintoday.RainTodayServiceManager`, `com.pushwoosh.local.BootReceiver`

3.6.2 Details

The following sections describe details about the test results of `RainToday . HD Regenradar` with version *1.5.1*.

App risks for enterprise usage

- Reasons for category privacy risks:
  - App Listing: Usage of detected functionality to access list of installed apps poses a privacy risk for detected app type.
- Reasons for category security risks:
  - Unprotected Web Content: App loads active web content (e.g. JavaScript or HTML files) without integrity protection. This poses a risk as man-in-the-middle attackers can modify the loaded web content and change the functionality of the app.

Communication security

- Client communication detected. The application can establish a network connection to one or more specific host systems. URLs with parameters found:

  - amzn://apps/android?p=
  - http://play.google.com/store/apps/details?id=
  - http://www.amazon.com/gp/mas/dl/android?p=
  - http://www.weatherpro.eu/fileadmin/weatherpro/pages.php?loadSection=
  - https://meteogroup.zendesk.com/hc/requests/new?ticket_form_id=44882
  - https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps
  - market://details?id=
  - market://details?id=com.google.android.gms.ads
  - market://search?q=pname:

- Communication endpoints is a list of all potential communication endpoints Appicaptor was able to detect. This allows quick enumeration of suspicious domains, raw IP Addresses, etc..
- Communication endpoints: .facebook.com, app.adjust.com, cdn.meteogroup.de, cp.pushwoosh.com, csi.gstatic.com, e.crashlytics.com, facebook.com, fb.me, feed.alertspro.meteogroup.com, googleads.g.doubleclick.net, graph-video.%s, graph.%s, maps.google.com, meteogroup.zendesk.com, pagead2.googlesyndication.com, play.google.com, plus.google.com, raintoday.weatherpro.de, settings.crashlytics.com, ssl.google-analytics.com, static.pushwoosh.com, webauth.meteogroup.de, www.amazon.com, www.google-analytics.com, www.google.com, www.weatherpro.eu
- App communicates with servers in 5 countries.
- Usage of SSL/TLS can protect the App's communication from adversaries. Tests indicate that communication is at least partly protected with SSL/TLS.
- Modifications of trust management found. Interface X509TrustManager is implemented or extended.
- Modifications of the SSL error handling detected: Class WebViewClient is extended and onReceivedSslError(...) is overwritten.

- The app loads the following HTML files via unprotected communication (http), which can be exploited by attackers to remotely change the displayed content and functionality of the app:
  - `http://play.google.com/store/apps/details?id=`
  - `http://play.google.com/store/apps/`
  - `http://static.pushwoosh.com/RichPush/Android/`
  - `http://maps.google.com/maps/api/staticmap?`
  - `http://feed.alertspro.meteogroup.com/AlertsPro/`
  - `http://www.weatherpro.eu/fileadmin/weatherpro/pages.php?loadSection=`
  - `http://www.amazon.com/gp/mas/dl/android?p=`
  - `http://cdn.meteogroup.de/images/mapengine/rain2.0/rad_%s/`
- The unprotected communication of the App via http connections can be eavesdroped or maliciously modified.
  - `http://play.google.com/store/apps/details?id=`
  - `http://www.amazon.com/gp/mas/dl/android?p=`
  - `http://www.weatherpro.eu/fileadmin/weatherpro/pages.php?loadSection=`

Data security

- The application requires the following permissions from the protection-level: NORMAL
  - VIBRATE (Allows access to the vibrator.)
  - ACCESS-NETWORK-STATE (Allows applications to access information about networks.)
  - READ-EXTERNAL-STORAGE (Allows an application to read from external storage. Any app that declares the WRITE-EXTERNAL-STORAGE permission is implicitly granted this permission. Currently, this permission is not enforced and all apps still have access to read from external storage without this permission. That will change in a future release and apps will require this permission to read from external storage. Note: If both minSdkVersion and targetSdkVersion

values are set to 3 or lower, the system implicitly grants this permission to the app.)

  - RECEIVE-BOOT-COMPLETED (Allows an application to receive the android.content.Intent ACTION-BOOT-COMPLETED that is broadcast after the system finishes booting. If you don't request this permission, you will not receive the broadcast at that time. Though holding this permission does not have any security implications, it can have a negative impact on the user experience by increasing the amount of time it takes the system to start and allowing applications to have themselves running without the user being aware of them. As such, you must explicitly declare your use of this facility to make that visible to the user.)
  - WAKE-LOCK (Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming.)
  - GET-ACCOUNTS (Allows access to the list of accounts in the Accounts Service.)

- The application requires the following permissions from the protectionlevel: DANGEROUS
  - INTERNET (Allows applications to open network sockets.)
  - ACCESS-FINE-LOCATION (Allows an app to access precise location from location sources such as GPS, cell towers, and Wi-Fi.)
  - READ-PHONE-STATE (Allows read only access to phone state. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
  - WRITE-EXTERNAL-STORAGE (Allows an application to write to external storage. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
  - ACCESS-COARSE-LOCATION (Allows an app to access approximate location derived from network location sources such as cell towers and Wi-Fi.)

- Application uses userdefined permissions. Application can access data of a foreign application which requires this permission to access data.
- Userdefined permission usage: `com.mg.raintoday.permission.RECEIVE-ADM-MESSAGE`, `com.amazon.device.messaging.permission.RECEIVE`, `com.mg.raintoday.permission.C2D-MESSAGE`, `com.android.vending.BILLING`, `com.google.android.c2dm.permission.RECEIVE`, `com.google.android.providers.gsf.permission.READ-GSERVICES`

- Application is propably overprivileged. Application has too much permissions. Foreign applications may be able to abuse this permission.
- Indicator for JavaScript bridge to Android API usage found. JavaScript used in the application (localy stored or loaded dynamicaly) may access and execute Android SDK API calls.
- Wifi-Direct is not enabled. There is no risk for exploiting a vulnerability in the wpa-supplicant module responsible for the wlan management. (http://www.coresecurity.com/advisories/android-wifi-direct-denial-service)

Input interface security

- No indicators for file handling found. The app does not define a filter scheme to process specific files.
- The app does not use protection measures for preventing screenshots. For apps displaying sensitive data it is recommended to disable screenshots.
- The application is vulnerable to tapjacking. When the protection is not used inside an exported activity another application is able to redirect touch events to the exported activity without the users consent.

Privacy

- The Application gathers a list of installed applications. Even though some legitimate applications may use this functionality, it can be misused to send this information to third parties.
- Code obfuscation techniques were detected for the app.
- Obfuscation levels are rated as LOW, MEDIUM, ABOVE MEDIUM, HIGH or UNKNOWN. The detected obfuscation level of HIGH provides sophisticated protection against manual analysis which requires a high effort and deep knowledge to reverse the functionality of the app.
- Device administration features not used.
- Application reads out different unique device Ids. These unique identifiers allows to identify the device and to distinguish it from other devices. Another option for reading out these IDs allow to determine the environment. The application can determine if it is running on a real device or on a virtual/emulated device.
- Accessed unique identifier(s): `build model`, `build manufacturer`, `build product`, `build serial`, `build display`, `build fingerprint`, `build brand`, `IMEI/MEID`, `SIM card serial`, `country code + mobile network code for SIM provider`, `unique Android ID`

- Indicators for usage of advertisement/tracking framework were found.
- The application contains components (Activities) which are exported. This means these parts of the application are accessible or executable by other applications. An external app can write or read information/data to or from this app. Additionally components of this application can be executed. Following Activities are exported:
  - `com.mg.raintoday.preferences.RainNotificationPrefActivity`
- In this application the allow backup option is enabled. This means the application and all application data will be included when performing a device backup. In case the application contains sensitive information these can be extracted from the backup archive or cloned onto other devices.
- Logging statements found in app. This might leak security or privacy relevant information.
- Permission READ-CONTACTS not used.
- Application reads information from different sensors. This allows the application to track the user and/or determine the environment of the user.
- World readable/writable preference files detected which can be read/written by other applications.
  - WORLD-READABLE

Runtime Security

- The application does not contain a scheduled alarm.
- Indicators found for dynamic code loading. The application loads executable code during runtime from a local or external source.
- Android dalvik code is loaded dynamically by the listed methods. Native code by Java Native Interface (for dynamic loading) is used.
- In the AndroidManifest.xml file the debuggable option is disabled. This prevents some attempts for debugging the application over the adb debug bridge with jdb. Depending of the used Android operating system this flag is not mandatory, in custom ROMs or rooted devices the OS may ignore this flag. On a non stock Android ROM this can still be misused for dynamic analyzes of the application or for doing runtime manipulation. This option should be disabled in released applications.
- The app is signed with a key that has a strength of 1024 bits. Google recommends to use a key with a strength of 2048 bit or more.
- Loadable libraries found:

- ARMv8 64 bit: lib/arm64-v8a/libRadarInterpolationNdk.so
- ARMv8 64 bit: lib/arm64-v8a/libcrashlytics-envelope.so
- ARMv8 64 bit: lib/arm64-v8a/libcrashlytics.so
- ARMv8 64 bit: lib/arm64-v8a/libunwind-crashlytics.so
- ARM 32 bit: lib/armeabi-v7a/libRadarInterpolationNdk.so
- ARM 32 bit: lib/armeabi-v7a/libcrashlytics-envelope.so
- ARM 32 bit: lib/armeabi-v7a/libcrashlytics.so
- ARM 32 bit: lib/armeabi-v7a/libunwind-crashlytics.so
- ARM 32 bit: lib/armeabi/libRadarInterpolationNdk.so
- ARM 32 bit: lib/armeabi/libcrashlytics.so
- MIPS I: lib/mips/libcrashlytics-envelope.so
- MIPS I: lib/mips/libcrashlytics.so
- MIPS I: lib/mips/libunwind-crashlytics.so
- MIPS I: lib/mips64/libcrashlytics-envelope.so
- MIPS I: lib/mips64/libcrashlytics.so
- MIPS I: lib/mips64/libunwind-crashlytics.so
- x86 32bit: lib/x86/libRadarInterpolationNdk.so
- x86 32bit: lib/x86/libcrashlytics-envelope.so
- x86 32bit: lib/x86/libcrashlytics.so
- x86 32bit: lib/x86/libunwind-crashlytics.so
- x86 64bit: lib/x86_64/libRadarInterpolationNdk.so

  - x86 64bit: lib/x86_64/libcrashlytics-envelope.so
  - x86 64bit: lib/x86_64/libcrashlytics.so
  - x86 64bit: lib/x86_64/libunwind-crashlytics.so

- The Application has the permission to start automatically after booting the device. The application can execute code without userinteraction or prevention.

Test Performance

- Execution time of all tests: 0:00:47.567

3.7 RegenRadar (Android)

3.7.1 Tests

The following Table 3.8 summarizes the results of the Android app `RegenRadar` with version *3.12.5*.

Table 3.8: Overview of summarized test results for »RegenRadar«

App risks for enterprise usage	
☒	*Implementation flaws? Yes.*
☒	*Privacy risks? Yes.*
☒	*Security risks? Yes.*
Blacklisted by policy	
☒	*Violations of default policy? Yes.*
Communication security	
☒	*Client communication used? Yes.*
☑	*Communication endpoints: 59 entries, see details.*
☑	*Communication with country: 7 entries, see details.*
☒	*SSL/TLS used? Yes.*
☑	*Domains accessed with http AND https:* `play.google.com`
☐	*Custom SSL/TLS trust manager implemented? No.*
☒	*SSL/TLS using custom error handling? Yes.*
☐	*SSL/TLS using faulty custom error handling? No.*
☐	*SSL/TLS using manual domain name verification? No.*
☒	*Unprotected HTML? Yes.*
☒	*Unprotected JavaScripts? Yes.*
☒	*Unprotected communication? Yes.*
Data security	

☑ *Cryptographic Primitives:* `"AES/CBC/PKCS5Padding"`
☒ *Application needs normal permissions? Yes.*
☒ *Application needs dangerous permissions? Yes.*
☑ *Userdefined permission usage:* `de.wetteronline.regenradar.permission.C2D-MESSAGE`, `com.google.android.c2dm.permission.RECEIVE`, `com.google.android.providers.gsf.permission.READ-GSERVICES`
☑ *Overprivileged permissions:* `READ-EXTERNAL-STORAGE`
☒ *Is application overprivileged? Yes.*
☒ *Application defines content provider? Yes.*
− *Content provider accessible without permission: None.*
☒ *JavaScript to SDK API bridge usage? Yes.*
☐ *WiFi-Direct enabled? No.*

Input interface security

− *App can handle documents of mimeType: None.*
☐ *Screenshot protection used? No.*
☐ *Tap Jacking Protection used? No.*

Privacy

☒ *Installed app list accessed? Yes.*
☒ *Obfuscation used? Yes.*
☑ *Obfuscation level is:* `HIGH`
− *Device administration policy entries: None.*
☑ *Accessed unique identifier(s): 12 entries, see details.*
☑ *Advertisment-/tracking frameworks found: 8 entries, see details.*
☒ *App provides public accessible activities? Yes.*
☒ *Backup of app is allowed? Yes.*
☒ *Log Statement Enabled? Yes.*
☐ *Permission to access address book? No.*
☒ *Remote auto backup with include enabled? Yes.*
☑ *Sensor usage:* `Camera (inactive)`, `WIFI-Based Location`, `GPS Location`, `Acceleration/Light`
☒ *Unprotected preference files found? Yes.*

Runtime Security

☒ *Scheduled Alarm Manager registered? Yes.*
☑ *Alarm repeating types:* `RTC`
☐ *Alarm intervals dynamically? No.*
☐ *Alarm Manager initialized dynamically? No.*
☒ *Dynamically loaded code at runtime? Yes.*
☑ *Dynamically loaded code at runtime type(s):* `dalvik.system.DexClassLoader(...)`, `ClassLoader.loadClass(...)`
☐ *Allow app debugging Flag? No.*
☑ *Executed component after Phone Reboot:* `de.wetteronline.lib.wetterapp.background.BackgroundReceiver`

3.7.2 Details

The following sections describe details about the test results of `RegenRadar` with version *3.12.5*.

App risks for enterprise usage

- Reasons for category implementation flaws:
  - Possible flaw: unintended use of insecure HTTP protocol for transmissions of parameters to servers capable of HTTPS.
- Reasons for category privacy risks:
  - Advertisement/Tracking: App uses more than 5 advertisement and tracking providers.
  - App Listing: Usage of detected functionality to access list of installed apps poses a privacy risk for detected app type.
- Reasons for category security risks:
  - Unprotected Web Content: App loads active web content (e.g. JavaScript or HTML files) without integrity protection. This poses a risk as man-in-the-middle attackers can modify the loaded web content and change the functionality of the app.

Blacklisted by policy

- Reasons for category violations of default policy:
  - Estimated overall app risk for the enterprise exceeds the security policy threshold due to detected risks and flaws exploitable by skilled attackers without the existence of additional supporting factors.

Communication security

- Client communication detected. The application can establish a network connection to one or more specific host systems. URLs with parameters found:
  - `amzn://apps/android?p=`
  - `amzn://apps/android?p=%s`
  - `amzn://apps/android?p=de.wetteronline.regenradar`

- amzn://apps/android?p=de.wetteronline.regenradarpro
- amzn://apps/android?p=de.wetteronline.wetterapp
- amzn://apps/android?p=de.wetteronline.wetterappamzn
- amzn://apps/android?p=de.wetteronline.wetterapppro
- amzn://apps/android?p=de.wetteronline.wettermaps
- flurry://flurrycall?event=
- flurry://flurrycall?event=adWillClose
- http://agof.de/datenschutz-allgemein/?lang=en
- http://m.wetteronline.de/android/?ADF=1
- http://m.wetteronline.de/android/?ADF=4
- http://m.wetteronline.de/cgi-bin/start?ADF=1
- http://m.wetteronline.de/cgi-bin/start?ADF=4
- http://play.google.com/store/apps/details?id=com.facebook.orca
- http://twitter.com/home?status=
- http://wetteronline.de/wetterticker?postId=
- http://www.amazon.de/gp/mas/dl/android?p=%s
- http://www.amazon.de/gp/mas/dl/android?p=de.wetteronline.regenradar
- http://www.amazon.de/gp/mas/dl/android?p=de.wetteronline.regenradarpro
- http://www.amazon.de/gp/mas/dl/android?p=de.wetteronline.wetterapp
- http://www.amazon.de/gp/mas/dl/android?p=de.wetteronline.wetterappamzn
- http://www.amazon.de/gp/mas/dl/android?p=de.wetteronline.wetterapppro
- http://www.amazon.de/gp/mas/dl/android?p=de.wetteronline.wettermaps

- http://www.wetteronline.at/?ireq=true&pid=p_search&searchpcid=external&searchstring=%s
- http://www.wetteronline.ch/?ireq=true&pid=p_search&searchpcid=external&searchstring=%s
- http://www.wetteronline.de/?ireq=true&pid=p_search&searchpcid=external&searchstring=%s
- http://www.wetteronline.de/datenschutz?lang=en
- https://m.google.com/app/plus/x/?v=compose&content=
- https://play.google.com/store/apps/details?id=
- https://play.google.com/store/apps/details?id=%s&referrer=utm_source3Dwetteronline.app26utm_medium3D%s
- https://www.facebook.com/dialog/feed?app_id=181821551957328&link=
- https://www.tumblr.com/oauth/authorize?oauth_token=%s
- market://details?id=
- market://details?id=%s
- market://details?id=%s&referrer=utm_source3Dwetteronline.app26utm_medium3D%s
- market://details?id=com.facebook.orca
- market://details?id=com.google.android.gms.ads
- market://details?id=de.wetteronline.regenradar&referrer=utm_source%3Dwetteronline.app%26utm_medium%3Dregenradar
- market://details?id=de.wetteronline.regenradarpro&referrer=utm_source%3Dwetteronline.app%26utm_medium%3Dregenradar
- market://details?id=de.wetteronline.wetterapp&referrer=utm_source%3Dwetteronline.app%26utm_medium%3Dregenradar

- market://details?id=de.wetteronline.
  wetterapppro&referrer=utm_source%
  3Dwetteronline.app%26utm_medium%3Dregenradar
- market://details?id=de.wetteronline.
  wettermaps&referrer=utm_source%
  3Dwetteronline.app%26utm_medium%3Dregenradar
- market://details?id=de.wetteronline.
  wetterticker&referrer=utm_source%
  3Dwetteronline.app%26utm_medium%3Dregenradar
- mraid://createCalendarEvent?event=
- mraid://open?url=
- mraid://playVideo?url=
- mraid://storePicture?url=
- ..https://play.google.com/store/apps/
  details?id=de.wetteronline.regenradar&
  referrer=utm_source%3Dwetteronline.app%
  26utm_medium%3Dregenrad
- ..https://play.google.com/store/apps/
  details?id=de.wetteronline.regenradarpro&
  referrer=utm_source%3Dwetteronline.app%
  26utm_medium%3Dregenrad
- ..https://play.google.com/store/apps/
  details?id=de.wetteronline.wetterapp&
  referrer=utm_source%3Dwetteronline.app%
  26utm_medium%3Dregenrad
- ..https://play.google.com/store/apps/
  details?id=de.wetteronline.wetterapppro&
  referrer=utm_source%3Dwetteronline.app%
  26utm_medium%3Dregenrad
- ..https://play.google.com/store/apps/
  details?id=de.wetteronline.wettermaps&
  referrer=utm_source%3Dwetteronline.app%
  26utm_medium%3Dregenrad
- ..https://play.google.com/store/apps/
  details?id=de.wetteronline.wetterticker&
  referrer=utm_source%3Dwetteronline.app%
  26utm_medium%3Dregenrad

- Communication endpoints is a list of all potential communication endpoints Appicaptor was able to detect. This allows quick enumeration of suspicious domains, raw IP Addresses, etc..
- Communication endpoints: `.facebook.com`, `a.applovin.com`, `adlog.flurry.com`, `ads.flurry.com`, `agof.de`, `amazon-adsystem.com`, `api-dev.wetteronline.de`, `api-stage.wetteronline.de`, `api.tumblr.com`, `api.wetteronline.de`, `app.getsentry.com`, `avr2.smaato.net`, `cdn.flurry.com`, `csi.gstatic.com`, `cv.apprupt.com`, `d.applovin.com`, `data.flurry.com`, `dwxjayoxbnyrr.cloudfront.net`, `facebook.com`, `googleads.g.doubleclick.net`, `graph-video.%s`, `graph.%s`, `graph.%s.facebook.com`, `graph.facebook.com`, `loghost.aatkit.com`, `m.google.com`, `m.wetteronline.de`, `mads.amazon-adsystem.com`, `mobile.smartadserver.com`, `ns.sascdn.com`, `pagead2.googlesyndication.com`, `play.google.com`, `plus.google.com`, `proton.flurry.com`, `rt.applovin.com`, `sb-ssl.google.com`, `soma-assets.smaato.net`, `soma.smaato.net`, `ssl.google-analytics.com`, `st.wetteronline.de`, `twitter.com`, `upload.wetteronline.de`, `vid.applovin.com`, `wetteronline.de`, `www.%s.facebook.com`, `www.agma-mmc.de`, `www.agof.de`, `www.amazon.de`, `www.facebook.com`, `www.google-analytics.com`, `www.google.com`, `www.googleapis.com`, `www.infonline.de`, `www.ivw.eu`, `www.tumblr.com`, `www.weatherandradar.com`, `www.wetteronline.at`, `www.wetteronline.ch`, `www.wetteronline.de`
- App communicates with servers in 7 countries.
- Communication with country: `Netherlands`, `United States`, `Ireland`, `United Kingdom`, `France`, `Germany`, `unknown`
- Usage of SSL/TLS can protect the App's communication from adversaries. Tests indicate that communication is at least partly protected with SSL/TLS.
- Mixed usage of HTTP and HTTPS: Protected and unprotected submission of parameters to the same domain. Indicates implementation flaw or weak communication protection.
- App uses the secure default SSL/TLS implementation for client communication. Error-prone modifications were not detected.
- Modifications of the SSL error handling detected: Class WebViewClient is extended and onReceivedSslError(...) is overwritten.

- The app loads the following HTML files via unprotected communication (http), which can be exploited by attackers to remotely change the displayed content and functionality of the app:
  - http://twitter.com/home?status=
  - http://rt.applovin.com/pix
  - http://www.wetteronline.de/apps#WetterTicker
  - http://www.wetteronline.de/uploader
  - http://www.wetteronline.ch/apps
  - http://www.wetteronline.ch/datenschutz/
  - http://www.wetteronline.ch/apps#WetterApp
  - http://www.wetteronline.at/apps
  - http://avr2.smaato.net/report2?
  - http://www.wetteronline.de/apps#RegenRadar
  - http://wetteronline.de/wetterticker?postId=
  - http://m.wetteronline.de/cgi-bin/start?ADF=1
  - http://www.wetteronline.at/datenschutz/
  - http://www.wetteronline.de/apps#WetterApp
  - http://www.wetteronline.ch/apps#WetterRadar
  - http://m.wetteronline.de/cgi-bin/start?ADF=4
  - http://www.wetteronline.de/datenschutz
  - http://www.wetteronline.ch/apps#RegenRadar
  - http://www.wetteronline.de/datenschutz/
  - http://m.wetteronline.de/android/?ADF=4
  - http://m.wetteronline.de/android/?ADF=1
  - http://soma.smaato.net/oapi/reqAd.jsp?
  - http://www.amazon.de/gp/mas/dl/android?p=%s
  - http://www.wetteronline.at/apps#WetterTicker
  - http://www.wetteronline.at/apps#RegenRadar
  - http://www.wetteronline.at/apps#WetterRadar
  - http://www.wetteronline.ch/uploader
  - http://www.wetteronline.de/mitgliedschaft

  - http://www.wetteronline.de/datenschutz?lang=en
  - http://www.wetteronline.at/mitgliedschaft
  - http://agof.de/datenschutz-allgemein/?lang=en
  - http://www.tumblr.com/connect/login_success.html
  - http://www.agof.de/datenschutz
  - http://www.wetteronline.ch/apps#WetterTicker
  - http://www.wetteronline.at/apps#WetterApp
  - http://www.wetteronline.de/apps#WetterRadar
  - http://www.wetteronline.de/apps
  - http://www.wetteronline.at/uploader
  - http://www.wetteronline.ch/mitgliedschaft

- The app loads the following JavaScript files via unprotected communication (http), which can be exploited by attackers to remotely change the displayed content and functionality of the app:
  - http://soma-assets.smaato.net/js/ormma.js
  - http://soma-assets.smaato.net/js/ormma_bridge.js

- The unprotected communication of the App via http connections can be eavesdroped or maliciously modified.
  - http://agof.de/datenschutz-allgemein/?lang=en
  - http://m.wetteronline.de/android/?ADF=1
  - http://m.wetteronline.de/android/?ADF=4
  - http://m.wetteronline.de/cgi-bin/start?ADF=1
  - http://m.wetteronline.de/cgi-bin/start?ADF=4
  - http://play.google.com/store/apps/details?id=com.facebook.orca
  - http://twitter.com/home?status=
  - http://wetteronline.de/wetterticker?postId=
  - http://www.amazon.de/gp/mas/dl/android?p=%s

- http://www.amazon.de/gp/mas/dl/android?p=de.wetteronline.regenradar
- http://www.amazon.de/gp/mas/dl/android?p=de.wetteronline.regenradarpro
- http://www.amazon.de/gp/mas/dl/android?p=de.wetteronline.wetterapp
- http://www.amazon.de/gp/mas/dl/android?p=de.wetteronline.wetterappamzn
- http://www.amazon.de/gp/mas/dl/android?p=de.wetteronline.wetterapppro
- http://www.amazon.de/gp/mas/dl/android?p=de.wetteronline.wettermaps
- http://www.wetteronline.at/?ireq=true&pid=p_search&searchpcid=external&searchstring=%s
- http://www.wetteronline.ch/?ireq=true&pid=p_search&searchpcid=external&searchstring=%s
- http://www.wetteronline.de/?ireq=true&pid=p_search&searchpcid=external&searchstring=%s
- http://www.wetteronline.de/datenschutz?lang=en

Data security

- The application requires the following permissions from the protection-level: NORMAL
  - WAKE-LOCK (Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming.)
  - ACCESS-WIFI-STATE (Allows applications to access information about Wi-Fi networks)
  - VIBRATE (Allows access to the vibrator.)
  - RECEIVE-BOOT-COMPLETED (Allows an application to receive the android.content.Intent ACTION-BOOT-COMPLETED that is broadcast after the system finishes booting. If you don't request this permission, you will not receive the broadcast at that time. Though holding this permission does not have any security implications, it can have a negative impact on the user experience by increasing the amount of time it takes the system to start and allowing applications to have themselves running without the user being aware of them. As such, you must explicitly declare your use of this facility to make that visible to the user.)

  - ACCESS-NETWORK-STATE (Allows applications to access information about networks.)
  - READ-EXTERNAL-STORAGE (Allows an application to read from external storage. Any app that declares the WRITE-EXTERNAL-STORAGE permission is implicitly granted this permission. Currently, this permission is not enforced and all apps still have access to read from external storage without this permission. That will change in a future release and apps will require this permission to read from external storage. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)

- The application requires the following permissions from the protection-level: DANGEROUS
  - ACCESS-FINE-LOCATION (Allows an app to access precise location from location sources such as GPS, cell towers, and Wi-Fi.)
  - WRITE-EXTERNAL-STORAGE (Allows an application to write to external storage. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
  - ACCESS-COARSE-LOCATION (Allows an app to access approximate location derived from network location sources such as cell towers and Wi-Fi.)
  - INTERNET (Allows applications to open network sockets.)
- Application uses userdefined permissions. Application can access data of a foreign application which requires this permission to access data.
- Application is propably overprivileged. Application has too much permissions. Foreign applications may be able to abuse this permission.
- The application uses a content provider for interacting with data set structures. Content providers are the standard interface that connects data in one process with code running in another process.
- Every ContentProvider defined in the application is protected by a permission. To access the interface from an external application it must request access to it. The interface is only available if an application defines these permissions.
- Indicator for JavaScript bridge to Android API usage found. JavaScript used in the application (localy stored or loaded dynamicaly) may access and execute Android SDK API calls.

- Wifi-Direct is not enabled. There is no risk for exploiting a vulnerability in the wpa-supplicant module responsible for the wlan management. (http://www.coresecurity.com/advisories/android-wifi-direct-denial-service)

Input interface security

- No indicators for file handling found. The app does not define a filter scheme to process specific files.
- The app does not use protection measures for preventing screenshots. For apps displaying sensitive data it is recommended to disable screenshots.
- The application is vulnerable to tapjacking. When the protection is not used inside an exported activity another application is able to redirect touch events to the exported activity without the users consent.

Privacy

- The Application gathers a list of installed applications. Even though some legitimate applications may use this functionality, it can be misused to send this information to third parties.
- Code obfuscation techniques were detected for the app.
- Obfuscation levels are rated as LOW, MEDIUM, ABOVE MEDIUM, HIGH or UNKNOWN. The detected obfuscation level of HIGH provides sophisticated protection against manual analysis which requires a high effort and deep knowledge to reverse the functionality of the app.
- Device administration features not used.
- Application reads out different unique device Ids. These unique identifiers allows to identify the device and to distinguish it from other devices. Another option for reading out these IDs allow to determine the environment. The application can determine if it is running on a real device or on a virtual/emulated device.
- Accessed unique identifier(s): `build model`, `build manufacturer`, `build product`, `build display`, `build fingerprint`, `build brand`, `IMEI/MEID`, `SIM card serial`, `Wifi-MAC address`, `country code + mobile network code for SIM provider`, `MMC (Mobile Country Code)`, `unique Android ID`
- Indicators for usage of advertisement/tracking framework were found.
- Advertisment-/tracking frameworks found: `Amazon Ad System`, `AppLovin`, `Crashlytics`, `Doubleclick`, `Flurry`, `Smaato`, `SmartAdServer`, `mopub`

- The application contains components (Activities) which are exported. This means these parts of the application are accessible or executable by other applications. An external app can write or read information/data to or from this app. Additionally components of this application can be executed. Following Activities are exported:
  - `de.wetteronline.wetterapp.widget.WidgetSnippetConfigure`
  - `com.facebook.CustomTabActivity`
- In this application the allow backup option is enabled. This means the application and all application data will be included when performing a device backup. In case the application contains sensitive information these can be extracted from the backup archive or cloned onto other devices.
- Logging statements found in app. This might leak security or privacy relevant information.
- Permission READ-CONTACTS not used.
- In this application full remote auto backup is enabled. There will be a remote backup of specified, possibly sensitive application data like database entries. The backup will be stored in the Google Cloud. The application defines the whitelisting of files in the backup configuration. The following specified files in the whitelisting will will be remotely stored in the Google Cloud:
  - database:WetterApp2.db
  - `sharedpref:de.wetteronline.regenradar_preferences.xml`
  - `sharedpref:de.wetteronline.regenradarpro_preferences.xml`
  - sharedpref:Einstellungen.xml
  - sharedpref:MainActivity.xml
  - sharedpref:PREFERENCES.xml
- Application reads information from different Sensors. This allows the application to track the user and/or determine the environment of the user. There was no Permission defined for camera usage, but the application contains specific API calls accessing the camera.Missing permissions despite of API calls could be an indication for missconfiguration or plugin/library code which is not used. For more detailed information application has to be reviewed manually.

- World readable/writable preference files detected which can be read/written by other applications.
  - WORLD-READABLE

Runtime Security

- The application contains a registered scheduled alarm. With such an alarm the application repeats the execution of the registered task for example every 10 hours. The following classes register scheduled tasks:
  - `de.wetteronline.lib.wetterapp.background.BackgroundReceiver`
  - `de.wetteronline.wetterapp.widget.AbstractWidgetProvider`
- The scheduled task gets repeated in the following intervals:
  - 1 minutes
  - 15 minutes
- The alarm manager has been initialized properly.
- Indicators found for dynamic code loading. The application loads executable code during runtime from a local or external source.
- Android dalvik code is loaded dynamically by the listed methods.
- In the AndroidManifest.xml file the debuggable option is disabled. This prevents some attempts for debugging the application over the adb debug bridge with jdb. Depending of the used Android operating system this flag is not mandatory, in custom ROMs or rooted devices the OS may ignore this flag. On a non stock Android ROM this can still be misused for dynamic analyzes of the application or for doing runtime manipulation. This option should be disabled in released applications.
- The Application has the permission to start automatically after booting the device. The application can execute code without userinteraction or prevention.

Test Performance

- Execution time of all tests: 0:01:05.630

3.8 Thermometer++ (Android)

3.8.1 Tests

The following Table 3.9 summarizes the results of the Android app `Thermometer++` with version *2.5.2*.

Table 3.9: Overview of summarized test results for »Thermometer++«

App risks for enterprise usage	
☐	*Implementation flaws? No.*
☐	*Privacy risks? No.*
☒	*Security risks? Yes.*
Blacklisted by policy	
☐	*Violations of default policy? No.*
Communication security	
☒	*Client communication used? Yes.*
☑	*Communication endpoints: 17 entries, see details.*
☑	*Communication with country:* `United States`, `Ireland`, `United Kingdom`
☒	*SSL/TLS used? Yes.*
☒	*Custom SSL/TLS trust manager implemented? Yes.*
☐	*Faulty custom SSL/TLS trust manager implemented? No.*
☒	*SSL/TLS using custom error handling? Yes.*
☐	*SSL/TLS using faulty custom error handling? No.*
☐	*SSL/TLS using manual domain name verification? No.*
☒	*Unprotected HTML? Yes.*
Data security	
☑	*Cryptographic Primitives:* `"AES/CBC/PKCS5Padding"`
☒	*Application needs normal permissions? Yes.*
☒	*Application needs dangerous permissions? Yes.*
☑	*Overprivileged permissions:* `READ_EXTERNAL_STORAGE`
☒	*Is application overprivileged? Yes.*
☒	*JavaScript to SDK API bridge usage? Yes.*
☐	*WiFi-Direct enabled? No.*
Input interface security	
⊟	*App can handle documents of mimeType: None.*
☐	*Screenshot protection used? No.*
☐	*Tap Jacking Protection used? No.*
Privacy	
☒	*Obfuscation used? Yes.*
☑	*Obfuscation level is:* `HIGH`
⊟	*Device administration policy entries: None.*

☑	*Accessed unique identifier(s): 7 entries, see details.*
☑	*Advertisment-/tracking frameworks found:* `Crashlytics`, `Doubleclick`, `Flurry`
☐	*App provides public accessible activities? No.*
☒	*Backup of app is allowed? Yes.*
☒	*Log Statement Enabled? Yes.*
☐	*Permission to access address book? No.*
☑	*Sensor usage:* `WIFI-Based Location`, `GPS Location`
☒	*Unprotected preference files found? Yes.*

Runtime Security

☐	*Scheduled Alarm Manager registered? No.*
☒	*Dynamically loaded code at runtime? Yes.*
☑	*Dynamically loaded code at runtime type(s):* `dalvik.system.DexClassLoader(...)`, `dalvik.system.PathClassLoader(...)`, `ClassLoader.loadClass(...)`
☐	*Allow app debugging Flag? No.*
☐	*Allow autoexecute after Phone Reboot? No.*
☒	*App uses outdated signature key? Yes.*

3.8.2 Details

The following sections describe details about the test results of `Thermometer++` with version *2.5.2*.

App risks for enterprise usage

- Reasons for category security risks:
  - Unprotected Web Content: App loads active web content (e.g. JavaScript or HTML files) without integrity protection. This poses a risk as man-in-the-middle attackers can modify the loaded web content and change the functionality of the app.

Communication security

- Client communication detected. The application can establish a network connection to one or more specific host systems. URLs with parameters found:
  - `http://%s/v3?lat=%s&lon=%s&cs=%s&source=android`
  - `https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps`
  - `market://details?id=`

  - market://details?id=com.google.android.gms.ads

- Communication endpoints is a list of all potential communication endpoints Appicaptor was able to detect. This allows quick enumeration of suspicious domains, raw IP Addresses, etc..
- Communication endpoints: apache.org, csi.gstatic.com, darksky.net, data.flurry.com, e.crashlytics.com, googleads.g.doubleclick.net, pagead2.googlesyndication.com, plus.google.com, proton.flurry.com, settings.crashlytics.com, ssl.google-analytics.com, worldweatheronline.com, wunderground.com, www.google-analytics.com, www.google.com, www.googleapis.com, www.googletagmanager.com
- App communicates with servers in 3 countries.
- Usage of SSL/TLS can protect the App's communication from adversaries. Tests indicate that communication is at least partly protected with SSL/TLS.
- Modifications of trust management found. Interface X509TrustManager is implemented or extended.
- Modifications of the SSL error handling detected: Class WebViewClient is extended and onReceivedSslError(...) is overwritten.
- The app loads the following HTML files via unprotected communication (http), which can be exploited by attackers to remotely change the displayed content and functionality of the app:
  - http://apache.org/xml/features/disallow-doctype-decl

Data security

- The application requires the following permissions from the protectionlevel: NORMAL
  - ACCESS-NETWORK-STATE (Allows applications to access information about networks.)
  - READ-EXTERNAL-STORAGE (Allows an application to read from external storage. Any app that declares the WRITE-EXTERNAL-STORAGE permission is implicitly granted this permission. Currently, this permission is not enforced and all apps still have access to read from external storage without this permission. That will change in a future release and apps will require this permission to read from external storage. Note: If both minSdkVersion and targetSdkVersion

values are set to 3 or lower, the system implicitly grants this permission to the app.)

  - WAKE-LOCK (Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming.)

- The application requires the following permissions from the protection-level: DANGEROUS

  - ACCESS-FINE-LOCATION (Allows an app to access precise location from location sources such as GPS, cell towers, and Wi-Fi.)
  - WRITE-EXTERNAL-STORAGE (Allows an application to write to external storage. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
  - ACCESS-COARSE-LOCATION (Allows an app to access approximate location derived from network location sources such as cell towers and Wi-Fi.)
  - INTERNET (Allows applications to open network sockets.)

- Application is propably overprivileged. Application has too much permissions. Foreign applications may be able to abuse this permission.
- Indicator for JavaScript bridge to Android API usage found. JavaScript used in the application (localy stored or loaded dynamicaly) may access and execute Android SDK API calls.
- Wifi-Direct is not enabled. There is no risk for exploiting a vulnerability in the wpa-supplicant module responsible for the wlan management. (http://www.coresecurity.com/advisories/android-wifi-direct-denial-service)

Input interface security

- No indicators for file handling found. The app does not define a filter scheme to process specific files.
- The app does not use protection measures for preventing screenshots. For apps displaying sensitive data it is recommended to disable screenshots.
- The application is vulnerable to tapjacking. When the protection is not used inside an exported activity another application is able to redirect touch events to the exported activity without the users consent.

Privacy

- Code obfuscation techniques were detected for the app.

- Obfuscation levels are rated as LOW, MEDIUM, ABOVE MEDIUM, HIGH or UNKNOWN. The detected obfuscation level of HIGH provides sophisticated protection against manual analysis which requires a high effort and deep knowledge to reverse the functionality of the app.
- Device administration features not used.
- Application reads out different unique device Ids. These unique identifiers allows to identify the device and to distinguish it from other devices. Another option for reading out these IDs allow to determine the environment. The application can determine if it is running on a real device or on a virtual/emulated device.
- Accessed unique identifier(s): `build model`, `build manufacturer`, `build product`, `build display`, `build fingerprint`, `build brand`, `unique Android ID`
- Indicators for usage of advertisement/tracking framework were found.
- The application contains no specific exported activity. The application has only launchable activities which are implicit exported. This means there are no activities which can be accessed by an external application. The start activity is:
  - `amuseworks.thermometer.MainActivity`
- In this application the allow backup option is enabled. This means the application and all application data will be included when performing a device backup. In case the application contains sensitive information these can be extracted from the backup archive or cloned onto other devices.
- Logging statements found in app. This might leak security or privacy relevant information.
- Permission READ-CONTACTS not used.
- Application reads information from different sensors. This allows the application to track the user and/or determine the environment of the user.
- World readable/writable preference files detected which can be read/written by other applications.
  - WORLD-READABLE

Runtime Security

- The application does not contain a scheduled alarm.
- Indicators found for dynamic code loading. The application loads executable code during runtime from a local or external source.
- Android dalvik code is loaded dynamically by the listed methods.

- In the AndroidManifest.xml file the debuggable option is disabled. This prevents some attempts for debugging the application over the adb debug bridge with jdb. Depending of the used Android operating system this flag is not mandatory, in custom ROMs or rooted devices the OS may ignore this flag. On a non stock Android ROM this can still be misused for dynamic analyzes of the application or for doing runtime manipulation. This option should be disabled in released applications.
- The app is signed with a key that has a strength of 1024 bits. Google recommends to use a key with a strength of 2048 bit or more.

Test Performance

- Execution time of all tests: 0:00:33.609

3.9 Transparent Clock & Wetter (Android)

3.9.1 Tests

The following Table 3.10 summarizes the results of the Android app `Transparent Clock & Wetter` with version *0.92.01.07*.

Table 3.10: Overview of summarized test results for »Transparent Clock & Wetter«

App risks for enterprise usage	
☒	*Implementation flaws? Yes.*
☒	*Privacy risks? Yes.*
☒	*Security risks? Yes.*
Blacklisted by policy	
☒	*Violations of default policy? Yes.*
Communication security	
☒	*Client communication used? Yes.*
☑	*Communication endpoints: 45 entries, see details.*
☑	*Communication with country: 8 entries, see details.*
☒	*SSL/TLS used? Yes.*
☑	*Domains accessed with http AND https:* `maps.googleapis.com`
☐	*Custom SSL/TLS trust manager implemented? No.*
☒	*SSL/TLS using custom error handling? Yes.*
☐	*SSL/TLS using faulty custom error handling? No.*
☐	*SSL/TLS using manual domain name verification? No.*
☒	*Unprotected HTML? Yes.*
☒	*Unprotected communication? Yes.*
Data security	
☑	*Cryptographic Primitives:* `"AES/CBC/PKCS5Padding"`

☒ *Application needs normal permissions? Yes.*
☒ *Application needs dangerous permissions? Yes.*
☑ *Userdefined permission usage:* `com.google.android.c2dm.permission.RECEIVE`, `com.droid27.transparentclockweather.permission.C2D-MESSAGE`
☑ *Overprivileged permissions:* `READ-EXTERNAL-STORAGE`
☒ *Is application overprivileged? Yes.*
☒ *Application defines content provider? Yes.*
− *Content provider accessible without permission: None.*
☒ *JavaScript to SDK API bridge usage? Yes.*
☒ i *JavaScript to SDK API bridge vulnerability? Yes. (see details)*
☐ *WiFi-Direct enabled? No.*

Input interface security

− *App can handle documents of mimeType: None.*
☐ *Screenshot protection used? No.*
☐ *Tap Jacking Protection used? No.*

Privacy

☒ *Installed app list accessed? Yes.*
☒ *Obfuscation used? Yes.*
☑ *Obfuscation level is:* `HIGH`
− *Device administration policy entries: None.*
☑ *Accessed unique identifier(s):* `build model`, `build manufacturer`, `build display`, `build fingerprint`, `unique Android ID`
☑ *Advertisment-/tracking frameworks found:* `Adcolony`, `Doubleclick`
☒ *App provides public accessible activities? Yes.*
☒ *Backup of app is allowed? Yes.*
☒ *Log Statement Enabled? Yes.*
☐ *Permission to access address book? No.*
☑ *Sensor usage:* `WIFI-Based Location`, `GPS Location`
☒ *Unprotected map queries? Yes.*
☒ *Unprotected preference files found? Yes.*

Runtime Security

☒ *Scheduled Alarm Manager registered? Yes.*
☑ *Alarm repeating types:* `RTC`, `RTC-WAKEUP`
☒ *Alarm intervals dynamically? Yes.*
☐ *Alarm Manager initialized dynamically? No.*
☒ *Dynamically loaded code at runtime? Yes.*
☑ *Dynamically loaded code at runtime type(s):* `dalvik.system.DexClassLoader(...)`, `dalvik.system.PathClassLoader(...)`, `ClassLoader.loadClass(...)`, `loadLibrary(...)`

☐ *Allow app debugging Flag? No.*
☒ *App uses outdated signature key? Yes.*
☑ *Executed component after Phone Reboot:* `com.droid27.transparentclockweather.receivers.BootCompletedReceiver`

3.9.2 Details

The following sections describe details about the test results of `Transparent Clock & Wetter` with version *0.92.01.07*.

App risks for enterprise usage

- Reasons for category implementation flaws:
  - Possible flaw: unintended use of insecure HTTP protocol for transmissions of parameters to servers capable of HTTPS.
  - Possible flaw: An application calling Android API methods by JavaScript and defining targetSdk version less than 17 could be vulnerable to remote code injection.
- Reasons for category privacy risks:
  - Unprotected Access: Disclosure of location or web query data though unprotected communication with service providers.
  - App Listing: Usage of detected functionality to access list of installed apps poses a privacy risk for detected app type.
- Reasons for category security risks:
  - Unprotected Web Content: App loads active web content (e.g. JavaScript or HTML files) without integrity protection. This poses a risk as man-in-the-middle attackers can modify the loaded web content and change the functionality of the app.

Blacklisted by policy

- Reasons for category violations of default policy:
  - Estimated overall app risk for the enterprise exceeds the security policy threshold due to detected risks and flaws exploitable by skilled attackers without the existence of additional supporting factors.

Communication security

- Client communication detected. The application can establish a network connection to one or more specific host systems. URLs with parameters found:
  - `http://autocomplete.wunderground.com/aq?query=`
  - `http://fonts.googleapis.com/css?family=Open+Sans:400,300,300italic,400italic,600,600italic,700,700italic,800,800italic&subset=latin,latin-ext\`
  - `http://maps.googleapis.com/maps/api/geocode/json?sensor=false&address=`
  - `http://market.android.com/details?id=com.droid27.transparentclockweather`
  - `http://market.android.com/details?id=com.droid27.weather.icons.pack01`
  - `http://market.android.com/details?id=com.droid27.weather.icons.pack02`
  - `http://pro.openweathermap.org/data/2.5/find?q=`
  - `http://pro.openweathermap.org/data/2.5/forecast/daily?mode=xml&cnt=16`
  - `http://pro.openweathermap.org/data/2.5/forecast?mode=xml`
  - `http://pro.openweathermap.org/data/2.5/weather?mode=xml`
  - `http://twitter.com/intent/user?screen_name=xdroid27`
  - `http://www.weatherunderground.com?apiref=dd0c2ef7cc832637`
  - `https://maps.googleapis.com/maps/api/geocode/json?latlng=%1$f,%2$f&sensor=true`
  - `https://maps.googleapis.com/maps/api/timezone/xml?sensor=false&location=`
  - `https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps`

  - https://play.google.com/store/apps/details?id=com.droid27.transparentclockweather
  - https://play.google.com/store/apps/details?id=com.droid27.transparentclockweather.premium
  - https://play.google.com/store/apps/developer?id=MACHAPP+Software+Ltd
  - market://details?id=
  - market://details?id=com.google.android.gms.ads

- Communication endpoints is a list of all potential communication endpoints Appicaptor was able to detect. This allows quick enumeration of suspicious domains, raw IP Addresses, etc..
- Communication endpoints: admob-app-id-7293982466.firebaseio.com, androidads23.adcolony.com, api.weather.com, api.wunderground.com, api.yr.no, app-measurement.com, autocomplete.wunderground.com, clients3.google.com, code.google.com, creativecommons.org, csi.gstatic.com, dmp.starbolt.io, fonts.googleapis.com, get.webgl.org, github.com, googleads.g.doubleclick.net, khronos.org, m.foreca.com, maps.googleapis.com, market.android.com, merlinthered.deviantart.com, my.mobfox.com, openweathermap.org, pagead2.googlesyndication.com, play.google.com, plus.google.com, pro.openweathermap.org, profiles.google.com, scripts.sil.org, sdk.starbolt.io, ssl.google-analytics.com, tcw.fcawx.net, themeforest.net, twitter.com, typodermicfonts.com, www.facebook.com, www.google-analytics.com, www.google.com, www.googletagmanager.com, www.ipanemagrafica.com, www.istockphoto.com, www.machapp.net, www.merrymeet.com, www.weatherunderground.com, www.yr.no
- App communicates with servers in 8 countries.
- Communication with country: Netherlands, United States, Norway, Ireland, Finland, Germany, unknown, Spain
- Usage of SSL/TLS can protect the App's communication from adversaries. Tests indicate that communication is at least partly protected with SSL/TLS.

- Mixed usage of HTTP and HTTPS: Protected and unprotected submission of parameters to the same domain. Indicates implementation flaw or weak communication protection.
- App uses the secure default SSL/TLS implementation for client communication. Error-prone modifications were not detected.
- Modifications of the SSL error handling detected: Class WebViewClient is extended and onReceivedSslError(...) is overwritten.
- The app loads the following HTML files via unprotected communication (http), which can be exploited by attackers to remotely change the displayed content and functionality of the app:
  - `http://pro.openweathermap.org/data/2.5/forecast/daily?mode=xml&cnt=16`
  - `http://pro.openweathermap.org/data/2.5/forecast?mode=xml`
  - `http://fonts.googleapis.com/css?family=Open+Sans:400,300,300italic,400italic,600,600italic,700,700italic,800,800italic&subset=latin,latin-ext\`
  - `http://my.mobfox.com/request.php`
  - `http://www.machapp.net/blog.php`
  - `http://www.facebook.com/transparentclockweather`
  - `http://typodermicfonts.com/coolvetica/`
  - `http://maps.googleapis.com/maps/api/geocode/json?sensor=false&address=`
  - `http://khronos.org/webgl/wiki/Getting_a_WebGL_Implementation`
  - `http://twitter.com/intent/user?screen_name=xdroid27`
  - `http://clients3.google.com/generate_204`
  - `http://autocomplete.wunderground.com/aq?query=`
  - `http://www.machapp.net/privacy_policy.php`
  - `http://scripts.sil.org/OFL`
  - `http://themeforest.net/licenses/terms/regular`

  - http://pro.openweathermap.org/data/2.5/find?q=
  - http://pro.openweathermap.org/data/2.5/weather?mode=xml
  - http://www.istockphoto.com/license.php

- The unprotected communication of the App via http connections can be eavesdroped or maliciously modified.
  - http://autocomplete.wunderground.com/aq?query=
  - http://fonts.googleapis.com/css?family=Open+Sans:400,300,300italic,400italic,600,600italic,700,700italic,800,800italic&subset=latin,latin-ext\
  - http://maps.googleapis.com/maps/api/geocode/json?sensor=false&address=
  - http://market.android.com/details?id=com.droid27.transparentclockweather
  - http://market.android.com/details?id=com.droid27.weather.icons.pack01
  - http://market.android.com/details?id=com.droid27.weather.icons.pack02
  - http://pro.openweathermap.org/data/2.5/find?q=
  - http://pro.openweathermap.org/data/2.5/forecast/daily?mode=xml&cnt=16
  - http://pro.openweathermap.org/data/2.5/forecast?mode=xml
  - http://pro.openweathermap.org/data/2.5/weather?mode=xml
  - http://twitter.com/intent/user?screen_name=xdroid27
  - http://www.weatherunderground.com?apiref=dd0c2ef7cc832637

Data security

- The application requires the following permissions from the protection-level: NORMAL

  - ACCESS-NETWORK-STATE (Allows applications to access information about networks.)
  - VIBRATE (Allows access to the vibrator.)
  - RECEIVE-BOOT-COMPLETED (Allows an application to receive the android.content.Intent ACTION-BOOT-COMPLETED that is broadcast after the system finishes booting. If you don't request this permission, you will not receive the broadcast at that time. Though holding this permission does not have any security implications, it can have a negative impact on the user experience by increasing the amount of time it takes the system to start and allowing applications to have themselves running without the user being aware of them. As such, you must explicitly declare your use of this facility to make that visible to the user.)
  - READ-EXTERNAL-STORAGE (Allows an application to read from external storage. Any app that declares the WRITE-EXTERNAL-STORAGE permission is implicitly granted this permission. Currently, this permission is not enforced and all apps still have access to read from external storage without this permission. That will change in a future release and apps will require this permission to read from external storage. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
  - WAKE-LOCK (Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming.)

- The application requires the following permissions from the protection-level: DANGEROUS
  - ACCESS-FINE-LOCATION (Allows an app to access precise location from location sources such as GPS, cell towers, and Wi-Fi.)
  - ACCESS-COARSE-LOCATION (Allows an app to access approximate location derived from network location sources such as cell towers and Wi-Fi.)
  - WRITE-EXTERNAL-STORAGE (Allows an application to write to external storage. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
  - READ-CALENDAR (Allows an application to read the user's calendar data.)
  - INTERNET (Allows applications to open network sockets.)
- Application uses userdefined permissions. Application can access data of a foreign application which requires this permission to access data.

- Application is propably overprivileged. Application has too much permissions. Foreign applications may be able to abuse this permission.
- The application uses a content provider for interacting with data set structures. Content providers are the standard interface that connects data in one process with code running in another process.
- Every ContentProvider defined in the application is protected by a permission. To access the interface from an external application it must request access to it. The interface is only available if an application defines these permissions.
- Indicator for JavaScript bridge to Android API usage found. JavaScript used in the application (localy stored or loaded dynamicaly) may access and execute Android SDK API calls.
- JavaScript to SDK API bridge vulnerability found: TargetSdk definition in the AndroidManifest.xml file is version: 12 . An application calling Android API methods by JavaScript and defining targetSdk version less than 17 could be vulnerable to remote code injection. For remote code injection the application has to load JavaScript or HTML code containing JavaScript code from a (generic) url.
- Wifi-Direct is not enabled. There is no risk for exploiting a vulnerability in the wpa-supplicant module responsible for the wlan management. (http://www.coresecurity.com/advisories/android-wifi-direct-denial-service)

Input interface security

- No indicators for file handling found. The app does not define a filter scheme to process specific files.
- The app does not use protection measures for preventing screenshots. For apps displaying sensitive data it is recommended to disable screenshots.
- The application is vulnerable to tapjacking. When the protection is not used inside an exported activity another application is able to redirect touch events to the exported activity without the users consent.

Privacy

- The Application gathers a list of installed applications. Even though some legitimate applications may use this functionality, it can be misused to send this information to third parties.
- Code obfuscation techniques were detected for the app.

- Obfuscation levels are rated as LOW, MEDIUM, ABOVE MEDIUM, HIGH or UNKNOWN. The detected obfuscation level of HIGH provides sophisticated protection against manual analysis which requires a high effort and deep knowledge to reverse the functionality of the app.
- Device administration features not used.
- Application reads out different unique device Ids. These unique identifiers allows to identify the device and to distinguish it from other devices. Another option for reading out these IDs allow to determine the environment. The application can determine if it is running on a real device or on a virtual/emulated device.
- Indicators for usage of advertisement/tracking framework were found.
- The application contains components (Activities) which are exported. This means these parts of the application are accessible or executable by other applications. An external app can write or read information/data to or from this app. Additionally components of this application can be executed. Following Activities are exported:
  - `com.droid27.transparentclockweather.preferences.QuickPreferencesActivity`
  - `com.droid27.transparentclockweather.LocationSetupActivity`
  - `com.droid27.weatherinterface.WeatherForecastActivity`
- In this application the allow backup option is enabled. This means the application and all application data will be included when performing a device backup. In case the application contains sensitive information these can be extracted from the backup archive or cloned onto other devices.
- Logging statements found in app. This might leak security or privacy relevant information.
- Permission READ-CONTACTS not used.
- Application reads information from different sensors. This allows the application to track the user and/or determine the environment of the user.
- App contains URL(s) that indicate an unprotected HTTP access to map providers. The transmitted location query parameters to the following map providers are in this case accesible by third parties:
  - Google Maps
- World readable/writable preference files detected which can be read/written by other applications.

  - WORLD-READABLE

Runtime Security

- The application contains a registered scheduled alarm. With such an alarm the application repeats the execution of the registered task for example every 10 hours. The following classes register scheduled tasks:
  - `com.droid27.transparentclockweather.z`
  - `com.droid27.transparentclockweather.receivers.d`
  - `com.droid27.transparentclockweather.receivers.b`
- The scheduled task gets repeated in the following intervals:
  - Dynamic interval(s)
  - 1 minutes
  - 1 hours
- The alarm manager has been initialized properly.
- Indicators found for dynamic code loading. The application loads executable code during runtime from a local or external source.
- Android dalvik code is loaded dynamically by the listed methods. Native code by Java Native Interface (for dynamic loading) is used.
- In the AndroidManifest.xml file the debuggable option is disabled. This prevents some attempts for debugging the application over the adb debug bridge with jdb. Depending of the used Android operating system this flag is not mandatory, in custom ROMs or rooted devices the OS may ignore this flag. On a non stock Android ROM this can still be misused for dynamic analyzes of the application or for doing runtime manipulation. This option should be disabled in released applications.
- The app is signed with a key that has a strength of 1024 bits. Google recommends to use a key with a strength of 2048 bit or more.
- The Application has the permission to start automatically after booting the device. The application can execute code without userinteraction or prevention.

Test Performance

- Execution time of all tests: 0:00:43.760

3.10 WarnWetter (Android)

3.10.1 Tests

The following Table 3.11 summarizes the results of the Android app `WarnWetter` with version *1.5*.

Table 3.11: Overview of summarized test results for »WarnWetter«

App risks for enterprise usage	
☐	*Implementation flaws? No.*
☐	*Privacy risks? No.*
☒	*Security risks? Yes.*
Blacklisted by policy	
☐	*Violations of default policy? No.*
Communication security	
☒	*Client communication used? Yes.*
☑	*Communication endpoints: 19 entries, see details.*
☑	*Communication with country:* `United States`, `Ireland`, `Switzerland`, `Germany`
☒	*SSL/TLS used? Yes.*
☐	*Custom SSL/TLS trust manager implemented? No.*
☐	*SSL/TLS using custom error handling? No.*
☒	*SSL/TLS using manual domain name verification? Yes.*
☒	*Unprotected HTML? Yes.*
☒	*Unprotected communication? Yes.*
Data security	
☑	*Cryptographic Primitives:* `"DES/ECB/NoPadding"`, `"RC4/NONE/NoPadding"`
☒	*Application needs normal permissions? Yes.*
☒	*Application needs dangerous permissions? Yes.*
☑	*Userdefined permission usage:* `de.dwd.warnapp.permission.C2D-MESSAGE`, `com.google.android.c2dm.permission.RECEIVE`
☑	*Overprivileged permissions:* `RECEIVE-BOOT-COMPLETED`
☒	*Is application overprivileged? Yes.*
☒	*Application defines content provider? Yes.*
−	*Content provider accessible without permission: None.*
☐	*WiFi-Direct enabled? No.*
Input interface security	
−	*App can handle documents of mimeType: None.*
☐	*Screenshot protection used? No.*
☐	*Tap Jacking Protection used? No.*

Privacy	
☒	*Obfuscation used? Yes.*
☑	*Obfuscation level is:* `HIGH`
⊟	*Device administration policy entries: None.*
☑	*Accessed unique identifier(s):* `build model`, `build product`, `build brand`, `IMEI/MEID`, `unique Android ID`
⊟	*Advertisment-/tracking frameworks found: None.*
☐	*App provides public accessible activities? No.*
☒	*Backup of app is allowed? Yes.*
☒	*Log Statement Enabled? Yes.*
☐	*Permission to access address book? No.*
☒	*Remote auto backup with exclude enabled? Yes.*
☑	*Sensor usage:* `GPS Location`
☒	*Unprotected preference files found? Yes.*

Runtime Security	
☐	*Scheduled Alarm Manager registered? No.*
☒	*Dynamically loaded code at runtime? Yes.*
☑	*Dynamically loaded code at runtime type(s):* `ClassLoader.loadClass(...)`, `loadLibrary(...)`
☐	*Allow app debugging Flag? No.*
☒	*Contains native libraries: Yes.*
☑	*Executed component after Phone Reboot:* `de.dwd.warnapp.gpspush.BackgroundLocationStarter`

3.10.2 Details

The following sections describe details about the test results of `WarnWetter` with version *1.5*.

App risks for enterprise usage

- Reasons for category security risks:
  - Unprotected Web Content: App loads active web content (e.g. JavaScript or HTML files) without integrity protection. This poses a risk as man-in-the-middle attackers can modify the loaded web content and change the functionality of the app.

Communication security

- Client communication detected. The application can establish a network connection to one or more specific host systems. URLs with parameters found:

  - http://www.lawinenwarndienst-bayern.de/infothek/verhaltenshinweise.php?rid=3
  - http://www.ubique.ch?app=dwd
  - http://www.youtube.com/watch?v=

- Communication endpoints is a list of all potential communication endpoints Appicaptor was able to detect. This allows quick enumeration of suspicious domains, raw IP Addresses, etc..
- Communication endpoints: accounts.google.com, app-measurement.com, app-prod-ws.warnwetter.de, crayx.ubique.ch, play.google.com, plus.google.com, s3-eu-west-1.amazonaws.com, s3.eu-central-1.amazonaws.com, ssl.google-analytics.com, www.bkg.bund.de, www.bsh.de, www.dwd.de, www.facebook.com, www.google-analytics.com, www.hochwasserzentralen.de, www.hochwasserzentralen.info, www.lawinenwarndienst-bayern.de, www.mhwz.de, www.ubique.ch
- App communicates with servers in 4 countries.
- Usage of SSL/TLS can protect the App's communication from adversaries. Tests indicate that communication is at least partly protected with SSL/TLS.
- App uses the secure default SSL/TLS implementation for client communication. Error-prone modifications were not detected.
- App uses the secure default error handling for SSL/TLS client communication. Error-prone modifications can be ruled out.
- Correct verification of the corresponding client hostname is important for SSL/TLS security. The app changes the secure default hostname verification by the following:
  - Interface HostnameVerifier is implemented or extended.
- The app loads the following HTML files via unprotected communication (http), which can be exploited by attackers to remotely change the displayed content and functionality of the app:
  - http://www.bsh.de/de/Meeresdaten/Vorhersagen/Sturmfluten/index.jsp
  - http://www.dwd.de/stellen
  - http://www.dwd.de/DE/leistungen/warnwetterapp/datenschutzerklaerung_app.html

  - http://www.hochwasserzentralen.info/lageberichte.htm
  - http://www.hochwasserzentralen.de/info.htm
  - http://www.dwd.de/DE/leistungen/gefahrenindizesthermisch/gefahrenindizesthermisch.html
  - http://www.lawinenwarndienst-bayern.de/lageberichte/
  - http://www.lawinenwarndienst-bayern.de/infothek/verhaltenshinweise.php?rid=3
  - http://www.hochwasserzentralen.de/lageberichte.htm
  - http://www.dwd.de/DE/leistungen/warnwetterapp/disclaimer_app.html
  - http://www.dwd.de/uvindex
  - http://play.google.com/store/apps/details
  - http://www.dwd.de/warnkriterien
- The unprotected communication of the App via http connections can be eavesdroped or maliciously modified.
  - http://www.lawinenwarndienst-bayern.de/infothek/verhaltenshinweise.php?rid=3
  - http://www.ubique.ch?app=dwd

Data security

- Usage of RC4 was identified. RC4 is a weak algorithm and it's use should be avoided.
- The application requires the following permissions from the protection-level: NORMAL
  - VIBRATE (Allows access to the vibrator.)
  - WAKE-LOCK (Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming.)
  - ACCESS-NETWORK-STATE (Allows applications to access information about networks.)

  - RECEIVE-BOOT-COMPLETED (Allows an application to receive the android.content.Intent ACTION-BOOT-COMPLETED that is broadcast after the system finishes booting. If you don't request this permission, you will not receive the broadcast at that time. Though holding this permission does not have any security implications, it can have a negative impact on the user experience by increasing the amount of time it takes the system to start and allowing applications to have themselves running without the user being aware of them. As such, you must explicitly declare your use of this facility to make that visible to the user.)

- The application requires the following permissions from the protection-level: DANGEROUS
  - INTERNET (Allows applications to open network sockets.)
  - ACCESS-FINE-LOCATION (Allows an app to access precise location from location sources such as GPS, cell towers, and Wi-Fi.)
- Application uses userdefined permissions. Application can access data of a foreign application which requires this permission to access data.
- Application is propably overprivileged. Application has too much permissions. Foreign applications may be able to abuse this permission.
- The application uses a content provider for interacting with data set structures. Content providers are the standard interface that connects data in one process with code running in another process.
- Every ContentProvider defined in the application is protected by a permission. To access the interface from an external application it must request access to it. The interface is only available if an application defines these permissions.
- Wifi-Direct is not enabled. There is no risk for exploiting a vulnerability in the wpa-supplicant module responsible for the wlan management. (http://www.coresecurity.com/advisories/android-wifi-direct-denial-service)

Input interface security

- No indicators for file handling found. The app does not define a filter scheme to process specific files.
- The app does not use protection measures for preventing screenshots. For apps displaying sensitive data it is recommended to disable screenshots.
- The application is vulnerable to tapjacking. When the protection is not used inside an exported activity another application is able to redirect touch events to the exported activity without the users consent.

Privacy

- Code obfuscation techniques were detected for the app.
- Obfuscation levels are rated as LOW, MEDIUM, ABOVE MEDIUM, HIGH or UNKNOWN. The detected obfuscation level of HIGH provides sophisticated protection against manual analysis which requires a high effort and deep knowledge to reverse the functionality of the app.
- Device administration features not used.
- Application reads out different unique device Ids. These unique identifiers allows to identify the device and to distinguish it from other devices. Another option for reading out these IDs allow to determine the environment. The application can determine if it is running on a real device or on a virtual/emulated device.
- No indicators for usage of advertisement/tracking framework were found.
- The application contains no specific exported activity. The application has only launchable activities which are implicit exported. This means there are no activities which can be accessed by an external application. The start activity is:
  - `de.dwd.warnapp.MainActivity`
- In this application the allow backup option is enabled. This means the application and all application data will be included when performing a device backup. In case the application contains sensitive information these can be extracted from the backup archive or cloned onto other devices.
- Logging statements found in app. This might leak security or privacy relevant information.
- Permission READ-CONTACTS not used.
- In this application full remote auto backup is enabled. There will be a full remote backup of almost all files created by the application. This includes database entries, shared preferences as well as files on local and external storage. The backup will be stored in the Google Cloud. All files are being remotely backuped except specified files which are excluded by blacklisting in the backup configuration. The application defines the following files are being excluded from the remote backup:
  - sharedpref:GCM.xml
- Application reads information from different sensors. This allows the application to track the user and/or determine the environment of the user.

- World readable/writable preference files detected which can be read/written by other applications.
  - WORLD-READABLE

Runtime Security

- The application does not contain a scheduled alarm.
- Indicators found for dynamic code loading. The application loads executable code during runtime from a local or external source.
- Android dalvik code is loaded dynamically by the listed methods. Native code by Java Native Interface (for dynamic loading) is used.
- In the AndroidManifest.xml file the debuggable option is disabled. This prevents some attempts for debugging the application over the adb debug bridge with jdb. Depending of the used Android operating system this flag is not mandatory, in custom ROMs or rooted devices the OS may ignore this flag. On a non stock Android ROM this can still be misused for dynamic analyzes of the application or for doing runtime manipulation. This option should be disabled in released applications.
- Loadable libraries found:
  - `ARM 32 bit: lib/armeabi-v7a/libdwd_shared.so`
  - `x86 32bit: lib/x86/libdwd_shared.so`
- The Application has the permission to start automatically after booting the device. The application can execute code without userinteraction or prevention.

Test Performance

- Execution time of all tests: 0:00:21.275

3.11 WeatherPro Free: Wetter gratis (Android)

3.11.1 Tests

The following Table 3.12 summarizes the results of the Android app `WeatherPro Free: Wetter gratis` with version *1.3*.

Table 3.12: Overview of summarized test results for »WeatherPro Free: Wetter gratis«

App risks for enterprise usage
☒ *Implementation flaws? Yes.*
☒ *Privacy risks? Yes.*

☒ *Security risks? Yes.*

Blacklisted by policy

☐ *Violations of default policy? No.*

Communication security

☒ *Client communication used? Yes.*
☑ *Communication endpoints: 41 entries, see details.*
☑ *Communication with country: 7 entries, see details.*
☒ *SSL/TLS used? Yes.*
☒ *Custom SSL/TLS trust manager implemented? Yes.*
☒ *Faulty custom SSL/TLS trust manager implemented? Yes.*
☒ *SSL/TLS using custom error handling? Yes.*
☐ *SSL/TLS using faulty custom error handling? No.*
☐ *SSL/TLS using manual domain name verification? No.*
☒ *Unprotected HTML? Yes.*
☒ *Unprotected communication? Yes.*

Data security

☑ *Cryptographic Primitives:* `"AES/CBC/PKCS5Padding"`
☒ *Application needs normal permissions? Yes.*
☒ *Application needs dangerous permissions? Yes.*
☑ *Userdefined permission usage: 6 entries, see details.*
☑ *Overprivileged permissions:* `GET_ACCOUNTS`, `READ_EXTERNAL_STORAGE`, `READ_PHONE_STATE`
☒ *Is application overprivileged? Yes.*
☒ *Application defines content provider? Yes.*
⊟ *Content provider accessible without permission: None.*
☒ *JavaScript to SDK API bridge usage? Yes.*
☐ *WiFi-Direct enabled? No.*

Input interface security

⊟ *App can handle documents of mimeType: None.*
☐ *Screenshot protection used? No.*
☐ *Tap Jacking Protection used? No.*

Privacy

☒ *Obfuscation used? Yes.*
☑ *Obfuscation level is:* `HIGH`
☑ *Obfuscation framework used:* `Proguard`
⊟ *Device administration policy entries: None.*
☑ *Accessed unique identifier(s): 8 entries, see details.*
☑ *Advertisment-/tracking frameworks found:* `Crashlytics`, `Doubleclick`
☒ *App provides public accessible activities? Yes.*
☐ *Backup of app is allowed? No.*
☒ *Log Statement Enabled? Yes.*

☐	*Permission to access address book? No.*
☑	*Sensor usage:* `Camera`, `WIFI-Based Location`, `Acceleration/Light`
☒	*Unprotected preference files found? Yes.*

Runtime Security	
☐	*Scheduled Alarm Manager registered? No.*
☒	*Dynamically loaded code at runtime? Yes.*
☑	*Dynamically loaded code at runtime type(s):* `dalvik.system.DexClassLoader(...)`, `ClassLoader.loadClass(...)`
☐	*Allow app debugging Flag? No.*
☒	*App uses outdated signature key? Yes.*
☑	*Executed component after Phone Reboot:* `com.mg.android.WeatherProServiceManager`

3.11.2 Details

The following sections describe details about the test results of `WeatherPro Free: Wetter gratis` with version *1.3*.

App risks for enterprise usage

- Reasons for category implementation flaws:
  - Possible flaw: App contains insecure code for communication protection with SSL/TLS. Common source for flawed communication protection against man-in-the-middle attacks.
- Reasons for category privacy risks:
  - Sensor Access: Usage of camera violates rules for detected app type and poses a potential risk by taking photos unnoticed or gaining access to those already stored.
- Reasons for category security risks:
  - Unprotected Web Content: App loads active web content (e.g. JavaScript or HTML files) without integrity protection. This poses a risk as man-in-the-middle attackers can modify the loaded web content and change the functionality of the app.

Communication security

- Client communication detected. The application can establish a network connection to one or more specific host systems. URLs with parameters found:

  - amzn://apps/android?p=
  - http://alertservice.weatherpro.meteogroup.de/service/AlertInfoFeed.php?language=%s&locale=%s
  - http://api.webcams.travel/rest?hl=en&method=wct.webcams.list_nearby&lat=#LAT#&lng=#LON#&radius=#RAD#&unit=km&per_page=#PPA#&page=#PAG#&format=json&devid=#DID#
  - http://apps.samsung.com/appquery/appDetail.as?appId=
  - http://play.google.com/store/apps/details?id=
  - http://www.amazon.com/gp/mas/dl/android?p=
  - http://www.amazon.de/gp/mas/dl/android?p=
  - http://www.weatherpro.eu/fileadmin/weatherpro/pages.php?loadSection=
  - https://meteogroup.zendesk.com/hc/requests/new?ticket_form_id=47132
  - https://meteogroup.zendesk.com/hc/requests/new?ticket_form_id=94845
  - market://details?id=
  - market://details?id=com.google.android.gms.ads
  - market://search?q=pname:

- Communication endpoints is a list of all potential communication endpoints Appicaptor was able to detect. This allows quick enumeration of suspicious domains, raw IP Addresses, etc..
- Communication endpoints: %s.%s, .facebook.com, alertservice.weatherpro.meteogroup.de, apache.org, api.netatmo.net, api.webcams.travel, app-measurement.com, app.adjust.com, apps.samsung.com, bit.ly, cdn.meteogroup.de, csi.gstatic.com, e.crashlytics.com, facebook.com, goo.gl, googleads.g.doubleclick.net, graph-video.%s, graph.%s, maps.google.com, mapservice.weatherpro.meteogroup.de, meteogroup-apps.firebaseio.com, meteogroup.zendesk.com, pagead2.googlesyndication.com, play.google.com, plus.google.com, sb-ssl.google.com, settings.crashlytics.com, ssl.google-analytics.

com, tile.openstreetmap.org, webauth.meteogroup.de, wetter24.de, www.amazon.com, www.amazon.de, www.google-analytics.com, www.google.com, www.googleapis.com, www.meteo24.de, www.meteogroup.com, www.tkqlhce.com, www.weatherpro.eu, www.wetter24.de

- App communicates with servers in 7 countries.
- Communication with country: Netherlands, United States, Ireland, United Kingdom, France, Switzerland, Germany
- Usage of SSL/TLS can protect the App's communication from adversaries. Tests indicate that communication is at least partly protected with SSL/TLS.
- Modifications of trust management found. Interface X509TrustManager is implemented or extended.
- The SSL trust management for socket communication is modified in an insecure way. The following implementations of the X509TrustManager interface should be checked:
  - Lcom/e/a/a/p.
- Modifications of the SSL error handling detected: Class WebViewClient is extended and onReceivedSslError(...) is overwritten.
- The app loads the following HTML files via unprotected communication (http), which can be exploited by attackers to remotely change the displayed content and functionality of the app:
  - http://www.amazon.de/gp/mas/dl/android?p=
  - http://play.google.com/store/apps/
  - http://wetter24.de/mein-wetter24de
  - http://cdn.meteogroup.de/images/mapengine/background/
  - http://bit.ly/wpandsn
  - http://maps.google.com/maps/api/staticmap?
  - http://%s.%s/weatherpro/%s?
  - http://www.weatherpro.eu/fileadmin/weatherpro/pages.php?loadSection=
  - http://apache.org/xml/features/nonvalidating/load-external-dtd

  - http://wetter24.de/mein-wetter24.de.html
  - http://play.google.com/store/apps/details?id=
  - http://bit.ly/wpandfree
  - http://cdn.meteogroup.de/images/wpro-android/wallpaper/
  - http://www.tkqlhce.com/click-7740252-12085164
  - http://www.wetter24.de/mein-wetter24de
  - http://www.wetter24.de/mein-wetter24de.html
  - http://alertservice.weatherpro.meteogroup.de/service/AlertInfoFeed.php?language=%s&locale=%s
  - http://www.amazon.com/gp/mas/dl/android?p=

- The unprotected communication of the App via http connections can be eavesdroped or maliciously modified.
  - http://alertservice.weatherpro.meteogroup.de/service/AlertInfoFeed.php?language=%s&locale=%s
  - http://api.webcams.travel/rest?hl=en&method=wct.webcams.list_nearby&lat=#LAT#&lng=#LON#&radius=#RAD#&unit=km&per_page=#PPA#&page=#PAG#&format=json&devid=#DID#
  - http://apps.samsung.com/appquery/appDetail.as?appId=
  - http://play.google.com/store/apps/details?id=
  - http://www.amazon.com/gp/mas/dl/android?p=
  - http://www.amazon.de/gp/mas/dl/android?p=
  - http://www.weatherpro.eu/fileadmin/weatherpro/pages.php?loadSection=

Data security

- The application requires the following permissions from the protection-level: NORMAL

  - GET-ACCOUNTS (Allows access to the list of accounts in the Accounts Service.)
  - READ-EXTERNAL-STORAGE (Allows an application to read from external storage. Any app that declares the WRITE-EXTERNAL-STORAGE permission is implicitly granted this permission. Currently, this permission is not enforced and all apps still have access to read from external storage without this permission. That will change in a future release and apps will require this permission to read from external storage. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
  - WAKE-LOCK (Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming.)
  - RECEIVE-BOOT-COMPLETED (Allows an application to receive the android.content.Intent ACTION-BOOT-COMPLETED that is broadcast after the system finishes booting. If you don't request this permission, you will not receive the broadcast at that time. Though holding this permission does not have any security implications, it can have a negative impact on the user experience by increasing the amount of time it takes the system to start and allowing applications to have themselves running without the user being aware of them. As such, you must explicitly declare your use of this facility to make that visible to the user.)
  - ACCESS-NETWORK-STATE (Allows applications to access information about networks.)

- The application requires the following permissions from the protection-level: DANGEROUS
  - ACCESS-COARSE-LOCATION (Allows an app to access approximate location derived from network location sources such as cell towers and Wi-Fi.)
  - WRITE-EXTERNAL-STORAGE (Allows an application to write to external storage. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
  - INTERNET (Allows applications to open network sockets.)
  - CAMERA (Required to be able to access the camera device. This will automatically enforce the uses-feature manifest element for all camera features. If you do not require all camera features or can properly operate if a camera is not available, then you must modify your manifest as appropriate in order to install on devices that don't support all camera features.)

  - READ-PHONE-STATE (Allows read only access to phone state. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)

- Application uses userdefined permissions. Application can access data of a foreign application which requires this permission to access data.
- Userdefined permission usage: `com.mg.android.free.permission.C2D-MESSAGE`, `com.android.vending.BILLING`, `com.mirrorlink.android.service.ACCESS-PERMISSION`, `com.android.vending.CHECK-LICENSE`, `com.google.android.permission.PROVIDE-BACKGROUND`, `com.google.android.c2dm.permission.RECEIVE`
- Application is propably overprivileged. Application has too much permissions. Foreign applications may be able to abuse this permission.
- The application uses a content provider for interacting with data set structures. Content providers are the standard interface that connects data in one process with code running in another process.
- Every ContentProvider defined in the application is protected by a permission. To access the interface from an external application it must request access to it. The interface is only available if an application defines these permissions.
- Indicator for JavaScript bridge to Android API usage found. JavaScript used in the application (localy stored or loaded dynamicaly) may access and execute Android SDK API calls.
- Wifi-Direct is not enabled. There is no risk for exploiting a vulnerability in the wpa-supplicant module responsible for the wlan management. (http://www.coresecurity.com/advisories/android-wifi-direct-denial-service)

Input interface security

- No indicators for file handling found. The app does not define a filter scheme to process specific files.
- The app does not use protection measures for preventing screenshots. For apps displaying sensitive data it is recommended to disable screenshots.
- The application is vulnerable to tapjacking. When the protection is not used inside an exported activity another application is able to redirect touch events to the exported activity without the users consent.

Privacy

- Code obfuscation techniques were detected for the app.

- Obfuscation levels are rated as LOW, MEDIUM, ABOVE MEDIUM, HIGH or UNKNOWN. The detected obfuscation level of HIGH provides sophisticated protection against manual analysis which requires a high effort and deep knowledge to reverse the functionality of the app.
- In general code obfuscation is done automatically by different obfuscation frameworks or obfuscation service providers. Detailed information to the detected framework Proguard can be found under: http://developer.android.com/tools/help/proguard.html
- Device administration features not used.
- Application reads out different unique device Ids. These unique identifiers allows to identify the device and to distinguish it from other devices. Another option for reading out these IDs allow to determine the environment. The application can determine if it is running on a real device or on a virtual/emulated device.
- Accessed unique identifier(s): `build model`, `build manufacturer`, `build product`, `build display`, `build fingerprint`, `build brand`, `Wifi-MAC address`, `unique Android ID`
- Indicators for usage of advertisement/tracking framework were found.
- The application contains components (Activities) which are exported. This means these parts of the application are accessible or executable by other applications. An external app can write or read information/data to or from this app. Additionally components of this application can be executed. Following Activities are exported:
  - `com.mg.weatherpro.LiveWallpaperSettings`
  - `com.mg.android.WidgetConfiguration`
  - `com.mg.weatherpro.preferences.ObsNotificationPrefActivity`
- In this application the allow backup option is disabled. This means no backup or restore of the application will ever be performed, even by a full-system backup that would otherwise cause all application data to be saved via adb backup function.
- Logging statements found in app. This might leak security or privacy relevant information.
- Permission READ-CONTACTS not used.
- Application reads information from different sensors. This allows the application to track the user and/or determine the environment of the user.

- World readable/writable preference files detected which can be read/written by other applications.
  - WORLD-READABLE

Runtime Security

- The application does not contain a scheduled alarm.
- Indicators found for dynamic code loading. The application loads executable code during runtime from a local or external source.
- Android dalvik code is loaded dynamically by the listed methods.
- In the AndroidManifest.xml file the debuggable option is disabled. This prevents some attempts for debugging the application over the adb debug bridge with jdb. Depending of the used Android operating system this flag is not mandatory, in custom ROMs or rooted devices the OS may ignore this flag. On a non stock Android ROM this can still be misused for dynamic analyzes of the application or for doing runtime manipulation. This option should be disabled in released applications.
- The app is signed with a key that has a strength of 1024 bits. Google recommends to use a key with a strength of 2048 bit or more.
- The Application has the permission to start automatically after booting the device. The application can execute code without userinteraction or prevention.

Test Performance

- Execution time of all tests: 0:00:39.434

3.12 Wetter & Uhr-Widget - Android (Android)

3.12.1 Tests

The following Table 3.13 summarizes the results of the Android app `Wetter & Uhr-Widget - Android` with version *5.9.1.2*.

Table 3.13: Overview of summarized test results for »Wetter & Uhr-Widget - Android«

App risks for enterprise usage
☒ *Implementation flaws? Yes.*
☒ *Privacy risks? Yes.*
☒ *Security risks? Yes.*
Blacklisted by policy
☒ *Violations of default policy? Yes.*

Communication security

- ☒ *Client communication used? Yes.*
- ☑ *Communication endpoints: 35 entries, see details.*
- ☑ *Communication with country: 6 entries, see details.*
- ☒ *SSL/TLS used? Yes.*
- ☑ *Domains accessed with http AND https:* `maps.googleapis.com`
- ☒ *Custom SSL/TLS trust manager implemented? Yes.*
- ☐ *Faulty custom SSL/TLS trust manager implemented? No.*
- ☒ *SSL/TLS using custom error handling? Yes.*
- ☐ *SSL/TLS using faulty custom error handling? No.*
- ☐ *SSL/TLS using manual domain name verification? No.*
- ☒ *Unprotected HTML? Yes.*
- ☒ *Unprotected JavaScripts? Yes.*
- ☒ *Unprotected communication? Yes.*

Data security

- ☑ *Cryptographic Primitives:* `"AES/CBC/PKCS5Padding", "RSA/NONE/NoPadding"`
- ☒ *Application needs normal permissions? Yes.*
- ☒ *Application needs dangerous permissions? Yes.*
- ☑ *Userdefined permission usage:* `com.google.android.permission.PROVIDE-BACKGROUND`, `com.devexpert.weather.permission.MAPS-RECEIVE`, `com.google.android.providers.gsf.permission.READ-GSERVICES`
- ☑ *Overprivileged permissions:* `READ-EXTERNAL-STORAGE`
- ☒ *Is application overprivileged? Yes.*
- ☒ *JavaScript to SDK API bridge usage? Yes.*
- ☐ *WiFi-Direct enabled? No.*

Input interface security

- ⊟ *App can handle documents of mimeType: None.*
- ☐ *Screenshot protection used? No.*
- ☐ *Tap Jacking Protection used? No.*

Privacy

- ☒ *Installed app list accessed? Yes.*
- ☒ *Obfuscation used? Yes.*
- ☑ *Obfuscation level is:* `HIGH`
- ⊟ *Device administration policy entries: None.*
- ☑ *Accessed unique identifier(s): 11 entries, see details.*
- ☑ *Advertisment-/tracking frameworks found: 6 entries, see details.*
- ☐ *App provides public accessible activities? No.*
- ☒ *Backup of app is allowed? Yes.*
- ☒ *Log Statement Enabled? Yes.*

☐	*Permission to access address book? No.*
☑	*Sensor usage:* `WIFI-Based Location`, `GPS Location`
☒	*Unprotected files found? Yes.*
☒	*Unprotected map queries? Yes.*

Runtime Security

☒	*Scheduled Alarm Manager registered? Yes.*
☑	*Alarm repeating types:* `ELAPSED-REALTIME`
☒	*Alarm intervals dynamically? Yes.*
☐	*Alarm Manager initialized dynamically? No.*
☒	*Dynamically loaded code at runtime? Yes.*
☑	*Dynamically loaded code at runtime type(s):* `dalvik.system.DexClassLoader(...)`, `ClassLoader.loadClass(...)`
☐	*Allow app debugging Flag? No.*
☒	*App uses outdated signature key? Yes.*
☑	*Executed component after Phone Reboot:* `com.devexpert.weather.controller.PackageReceiver`

3.12.2 Details

The following sections describe details about the test results of `Wetter & Uhr-Widget - Android` with version *5.9.1.2*.

App risks for enterprise usage

- Reasons for category implementation flaws:
  - Possible flaw: unintended use of insecure HTTP protocol for transmissions of parameters to servers capable of HTTPS.
- Reasons for category privacy risks:
  - Advertisement/Tracking: App uses more than 5 advertisement and tracking providers.
  - Unprotected Access: Disclosure of location or web query data though unprotected communication with service providers.
  - App Listing: Usage of detected functionality to access list of installed apps poses a privacy risk for detected app type.
- Reasons for category security risks:
  - Unprotected Web Content: App loads active web content (e.g. JavaScript or HTML files) without integrity protection. This poses a risk as man-in-the-middle attackers can modify the loaded web content and change the functionality of the app.

Blacklisted by policy

- Reasons for category violations of default policy:
  - Estimated overall app risk for the enterprise exceeds the security policy threshold due to detected risks and flaws exploitable by skilled attackers without the existence of additional supporting factors.

Communication security

- Client communication detected. The application can establish a network connection to one or more specific host systems. URLs with parameters found:
  - `http://devexpert.fcawx.net/?format=xml&units=imperial&`
  - `http://m.foreca.com?ref=devexpert`
  - `http://m.foreca.com?ref=devexpert&l=`
  - `http://maps.googleapis.com/maps/api/geocode/json?address=`
  - `http://maps.googleapis.com/maps/api/geocode/json?latlng=`
  - `http://www.myweather2.com/activity/current-weather.aspx?rt=latlon&lat=`
  - `https://maps.googleapis.com/maps/api/js?signed_in=true&language=`
  - `https://maps.googleapis.com/maps/api/timezone/xml?sensor=false&timestamp=`
  - `https://play.google.com/store/apps/details?id=`
  - `market://details?id=`
  - `market://details?id=%s`
  - `market://details?id=com.devexpert.weatheradfree`
  - `market://details?id=com.google.android.gm`
  - `market://details?id=com.google.android.gms.ads`
  - `market://search?q=pub:Devexpert.NET`

- Communication endpoints is a list of all potential communication endpoints Appicaptor was able to detect. This allows quick enumeration of suspicious domains, raw IP Addresses, etc..
- Communication endpoints: `ad6.%s.liverail.com`, `ad6.liverail.com`, `ads.rubiconproject.com`, `amazon-adsystem.amazon.com`, `amazon-adsystem.com`, `analytics.mopub.com`, `api.pubnative.net`, `app.getsentry.com`, `applift-a.apptornado.com`, `applift-a.apptornado.com`, `http`, `avr.smaato.net`, `devexpert.fcawx.net`, `devexpert.weatherunlocked.com`, `googleads.g.doubleclick.net`, `graph.%s.facebook.com`, `graph.facebook.com`, `m.foreca.com`, `maps.googleapis.com`, `market.android.com`, `play.google.com`, `plus.google.com`, `rri.appodeal.com`, `s3.amazonaws.com`, `sdk.appbrain.com`, `http`, `soma-assets.smaato.net`, `soma.smaato.net`, `twitter.com`, `www.%s.facebook.com`, `www.appodealx.com`, `www.devexpert.net`, `www.facebook.com`, `www.google.com`, `www.googleapis.com`, `www.mopub.com`, `www.myweather2.com`
- App communicates with servers in 6 countries.
- Communication with country: `United States`, `Ireland`, `Finland`, `United Kingdom`, `Germany`, `unknown`
- Usage of SSL/TLS can protect the App's communication from adversaries. Tests indicate that communication is at least partly protected with SSL/TLS.
- Mixed usage of HTTP and HTTPS: Protected and unprotected submission of parameters to the same domain. Indicates implementation flaw or weak communication protection.
- Modifications of trust management found. Interface X509TrustManager is implemented or extended.
- Modifications of the SSL error handling detected: Class WebViewClient is extended and onReceivedSslError(...) is overwritten.
- The app loads the following HTML files via unprotected communication (http), which can be exploited by attackers to remotely change the displayed content and functionality of the app:
  - `http://www.devexpert.net/weather/faq`
  - `http://devexpert.weatherunlocked.com/api/weather/`
  - `http://maps.googleapis.com/maps/api/geocode/json?address=`

  - `http://maps.googleapis.com/maps/api/geocode/json?latlng=`
  - `http://avr.smaato.net/report`
  - `http://www.appodealx.com/complains`
  - `http://www.myweather2.com/activity/current-weather.aspx?rt=latlon&lat=`
  - `http://soma.smaato.net/oapi/reqAd.jsp?`

- The app loads the following JavaScript files via unprotected communication (http), which can be exploited by attackers to remotely change the displayed content and functionality of the app:
  - `http://soma-assets.smaato.net/js/ormma.js`
  - `http://ads.rubiconproject.com/ad/12530.js`
  - `http://soma-assets.smaato.net/js/ormma_bridge.js`
- The unprotected communication of the App via http connections can be eavesdroped or maliciously modified.
  - `http://devexpert.fcawx.net/?format=xml&units=imperial&`
  - `http://m.foreca.com?ref=devexpert`
  - `http://m.foreca.com?ref=devexpert&l=`
  - `http://maps.googleapis.com/maps/api/geocode/json?address=`
  - `http://maps.googleapis.com/maps/api/geocode/json?latlng=`
  - `http://www.myweather2.com/activity/current-weather.aspx?rt=latlon&lat=`

Data security

- Usage of RSA was identified. RSA without padding is considered weak.
- The application requires the following permissions from the protection-level: NORMAL
  - ACCESS-NETWORK-STATE (Allows applications to access information about networks.)

  - READ-EXTERNAL-STORAGE (Allows an application to read from external storage. Any app that declares the WRITE-EXTERNAL-STORAGE permission is implicitly granted this permission. Currently, this permission is not enforced and all apps still have access to read from external storage without this permission. That will change in a future release and apps will require this permission to read from external storage. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
  - WAKE-LOCK (Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming.)
  - VIBRATE (Allows access to the vibrator.)
  - RECEIVE-BOOT-COMPLETED (Allows an application to receive the android.content.Intent ACTION-BOOT-COMPLETED that is broadcast after the system finishes booting. If you don't request this permission, you will not receive the broadcast at that time. Though holding this permission does not have any security implications, it can have a negative impact on the user experience by increasing the amount of time it takes the system to start and allowing applications to have themselves running without the user being aware of them. As such, you must explicitly declare your use of this facility to make that visible to the user.)

- The application requires the following permissions from the protection-level: DANGEROUS
  - READ-CALENDAR (Allows an application to read the user's calendar data.)
  - INTERNET (Allows applications to open network sockets.)
  - WRITE-EXTERNAL-STORAGE (Allows an application to write to external storage. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
  - ACCESS-COARSE-LOCATION (Allows an app to access approximate location derived from network location sources such as cell towers and Wi-Fi.)
  - ACCESS-FINE-LOCATION (Allows an app to access precise location from location sources such as GPS, cell towers, and Wi-Fi.)
- Application uses userdefined permissions. Application can access data of a foreign application which requires this permission to access data.
- Application is propably overprivileged. Application has too much permissions. Foreign applications may be able to abuse this permission.

- Indicator for JavaScript bridge to Android API usage found. JavaScript used in the application (localy stored or loaded dynamicaly) may access and execute Android SDK API calls.
- Wifi-Direct is not enabled. There is no risk for exploiting a vulnerability in the wpa-supplicant module responsible for the wlan management. (http://www.coresecurity.com/advisories/android-wifi-direct-denial-service)

Input interface security

- No indicators for file handling found. The app does not define a filter scheme to process specific files.
- The app does not use protection measures for preventing screenshots. For apps displaying sensitive data it is recommended to disable screenshots.
- The application is vulnerable to tapjacking. When the protection is not used inside an exported activity another application is able to redirect touch events to the exported activity without the users consent.

Privacy

- The Application gathers a list of installed applications. Even though some legitimate applications may use this functionality, it can be misused to send this information to third parties.
- Code obfuscation techniques were detected for the app.
- Obfuscation levels are rated as LOW, MEDIUM, ABOVE MEDIUM, HIGH or UNKNOWN. The detected obfuscation level of HIGH provides sophisticated protection against manual analysis which requires a high effort and deep knowledge to reverse the functionality of the app.
- Device administration features not used.
- Application reads out different unique device Ids. These unique identifiers allows to identify the device and to distinguish it from other devices. Another option for reading out these IDs allow to determine the environment. The application can determine if it is running on a real device or on a virtual/emulated device.
- Accessed unique identifier(s): `build model`, `build manufacturer`, `build product`, `build hardware`, `build display`, `build brand`, `IMEI/MEID`, `Wifi-MAC address`, `country code + mobile network code for SIM provider`, `MMC (Mobile Country Code)`, `unique Android ID`
- Indicators for usage of advertisement/tracking framework were found.

- Advertisment-/tracking frameworks found: `Amazon Ad System`, `Appbrain`, `Doubleclick`, `LiveRail`, `Smaato`, `mopub`
- The application contains no specific exported activity. The application has only launchable activities which are implicit exported. This means there are no activities which can be accessed by an external application. The start activity is:
  - `com.devexpert.weather.view.HomeActivity`
- In this application the allow backup option is enabled. This means the application and all application data will be included when performing a device backup. In case the application contains sensitive information these can be extracted from the backup archive or cloned onto other devices.
- Logging statements found in app. This might leak security or privacy relevant information.
- Permission READ-CONTACTS not used.
- Application reads information from different sensors. This allows the application to track the user and/or determine the environment of the user.
- World readable/writable files detected which can be read/written by other applications.
  - WORLD-READABLE
- App contains URL(s) that indicate an unprotected HTTP access to map providers. The transmitted location query parameters to the following map providers are in this case accesible by third parties:
  - Google Maps

Runtime Security

- The application contains a registered scheduled alarm. With such an alarm the application repeats the execution of the registered task for example every 10 hours. The following classes register scheduled tasks:
  - `com.appbrain.a.cm`
- The scheduled task gets repeated in the following intervals:
  - Dynamic interval(s)
- The alarm manager has been initialized properly.
- Indicators found for dynamic code loading. The application loads executable code during runtime from a local or external source.

- Android dalvik code is loaded dynamically by the listed methods.
- In the AndroidManifest.xml file the debuggable option is disabled. This prevents some attempts for debugging the application over the adb debug bridge with jdb. Depending of the used Android operating system this flag is not mandatory, in custom ROMs or rooted devices the OS may ignore this flag. On a non stock Android ROM this can still be misused for dynamic analyzes of the application or for doing runtime manipulation. This option should be disabled in released applications.
- The app is signed with a key that has a strength of 1024 bits. Google recommends to use a key with a strength of 2048 bit or more.
- The Application has the permission to start automatically after booting the device. The application can execute code without userinteraction or prevention.

Test Performance

- Execution time of all tests: 0:00:51.692

3.13 Wetter Deutschland XL PRO (Android)

3.13.1 Tests

The following Table 3.14 summarizes the results of the Android app `Wetter Deutschland XL PRO` with version *1.4.0*.

Table 3.14: Overview of summarized test results for »Wetter Deutschland XL PRO«

App risks for enterprise usage	
☐	*Implementation flaws? No.*
☒	*Privacy risks? Yes.*
☒	*Security risks? Yes.*
Blacklisted by policy	
☐	*Violations of default policy? No.*
Communication security	
☒	*Client communication used? Yes.*
☑	*Communication endpoints: 46 entries, see details.*
☑	*Communication with country:* `Canada`, `United States`, `Ireland`, `France`, `unknown`
☒	*SSL/TLS used? Yes.*
☒	*Custom SSL/TLS trust manager implemented? Yes.*
☐	*Faulty custom SSL/TLS trust manager implemented? No.*
☒	*SSL/TLS using custom error handling? Yes.*
☐	*SSL/TLS using faulty custom error handling? No.*

☐ *SSL/TLS using manual domain name verification? No.*
☒ *Unprotected HTML? Yes.*
☒ *Unprotected communication? Yes.*

Data security

☑ *Cryptographic Primitives:* `"AES/CBC/PKCS5Padding"`
☒ *Application needs normal permissions? Yes.*
☒ *Application needs dangerous permissions? Yes.*
☑ *Userdefined permission usage:* `com.exovoid.weather.app.permission.C2D-MESSAGE`, `com.android.vending.BILLING`, `com.google.android.c2dm.permission.RECEIVE`, `com.google.android.providers.gsf.permission.READ-GSERVICES`
☐ *Is application overprivileged? No.*
☒ *Application defines content provider? Yes.*
⊟ *Content provider accessible without permission: None.*
☒ *JavaScript to SDK API bridge usage? Yes.*
☐ *WiFi-Direct enabled? No.*

Input interface security

⊟ *App can handle documents of mimeType: None.*
☐ *Screenshot protection used? No.*
☐ *Tap Jacking Protection used? No.*

Privacy

☒ *Obfuscation used? Yes.*
☑ *Obfuscation level is:* `HIGH`
⊟ *Device administration policy entries: None.*
☑ *Accessed unique identifier(s): 9 entries, see details.*
☑ *Advertisment-/tracking frameworks found:* `Doubleclick`, `LiveRail`, `mopub`
☒ *App provides public accessible activities? Yes.*
☒ *Backup of app is allowed? Yes.*
☒ *Log Statement Enabled? Yes.*
☐ *Permission to access address book? No.*
☑ *Sensor usage:* `GPS Location`, `Acceleration/Light`
☒ *Unprotected files found? Yes.*
☒ *Unprotected map queries? Yes.*
☒ *Unprotected preference files found? Yes.*

Runtime Security

☒ *Scheduled Alarm Manager registered? Yes.*
☑ *Alarm repeating types:* `RTC`
☒ *Alarm intervals dynamically? Yes.*
☐ *Alarm Manager initialized dynamically? No.*
☒ *Dynamically loaded code at runtime? Yes.*

☑ *Dynamically loaded code at runtime type(s):* `dalvik.system.DexClassLoader(...)`, `ClassLoader.loadClass(...)`, `load(...)`, `loadLibrary(...)`
☐ *Allow app debugging Flag? No.*
☒ *Contains native libraries: Yes.*
☑ *Executed component after Phone Reboot:* `com.exovoid.weather.app.RefreshBroadcastReceiver`

3.13.2 Details

The following sections describe details about the test results of `Wetter Deutschland XL PRO` with version *1.4.0*.

App risks for enterprise usage

- Reasons for category privacy risks:
  - Unprotected Access: Disclosure of location or web query data though unprotected communication with service providers.
- Reasons for category security risks:
  - Unprotected Web Content: App loads active web content (e.g. JavaScript or HTML files) without integrity protection. This poses a risk as man-in-the-middle attackers can modify the loaded web content and change the functionality of the app.

Communication security

- Client communication detected. The application can establish a network connection to one or more specific host systems. URLs with parameters found:
  - `amzn://apps/android?p=`
  - `http://droidexp-featured.appspot.com/listappfromexo?lang=`
  - `http://fonts.googleapis.com/css?family=Open+Sans:400,300,300italic,400italic,600,600italic,700,700italic,800,800italic&subset=latin,latin-ext\`
  - `http://maps.googleapis.com/maps/api/geocode/json?address=`
  - `http://maps.googleapis.com/maps/api/geocode/json?latlng=`

  - http://play.google.com/store/apps/details?id=com.facebook.orca
  - http://share.weatherxl.com/?b=
  - http://www.wunderground.com/?apiref=6b82b4478782f4bf
  - https://mobilecrashreporting.googleapis.com/v1/crashes:batchCreate?key=
  - market://details?id=
  - market://details?id=%s
  - market://details?id=com.facebook.orca
  - market://details?id=com.google.android.gms.ads

- Communication endpoints is a list of all potential communication endpoints Appicaptor was able to detect. This allows quick enumeration of suspicious domains, raw IP Addresses, etc..
- Communication endpoints: .facebook.com, ad6.%s.liverail.com, ad6.liverail.com, analytics.mopub.com, app-measurement.com, buzzingandroid.com, csi.gstatic.com, dmp.starbolt.io, droidexp-featured.appspot.com, facebook.com, fonts.googleapis.com, get.webgl.org, goo.gl, googleads.g.doubleclick.net, graph-video.%s, graph.%s, graph.%s.facebook.com, graph.facebook.com, i.smte.ch, khronos.org, maps.googleapis.com, mobilecrashreporting.googleapis.com, my.mobfox.com, nineoldandroids.com, pagead2.googlesyndication.com, play.google.com, plus.google.com, sb-ssl.google.com, sdk.starbolt.io, share.weatherxl.com, storage.googleapis.com, twitter.com, weather-xl.firebaseio.com, weathergae.exovoid.ch, weathergaeimg.exovoid.ch, weatherpxauto.xvo.ch, weatherpxbackup.xvo.ch, www.%s.facebook.com, www.exovoid.ch, www.facebook.com, www.google.com, www.googleapis.com, www.mopub.com, www.smallte.ch, www.wunderground.com, xvo.ch
- App communicates with servers in 5 countries.
- Usage of SSL/TLS can protect the App's communication from adversaries. Tests indicate that communication is at least partly protected with SSL/TLS.
- Modifications of trust management found. Interface X509TrustManager is implemented or extended.

- Modifications of the SSL error handling detected: Class WebViewClient is extended and onReceivedSslError(...) is overwritten.
- The app loads the following HTML files via unprotected communication (http), which can be exploited by attackers to remotely change the displayed content and functionality of the app:
  - `http://weatherpxauto.xvo.ch/weatherimages`
  - `http://i.smte.ch/icondrawer`
  - `http://i.smte.ch/localize`
  - `http://fonts.googleapis.com/css?family=Open+Sans:400,300,300italic,400italic,600,600italic,700,700italic,800,800italic&subset=latin,latin-ext\`
  - `http://my.mobfox.com/request.php`
  - `http://www.smallte.ch/appicons/`
  - `http://weatherpxbackup.xvo.ch/weatherimages`
  - `http://xvo.ch/weather`
  - `http://droidexp-featured.appspot.com/listappfromexo?lang=`
  - `http://maps.googleapis.com/maps/api/geocode/json?latlng=`
  - `http://weatherpxbackup.xvo.ch/l2g`
  - `http://storage.googleapis.com/weather_lat_geoid`
  - `http://khronos.org/webgl/wiki/Getting_a_WebGL_Implementation`
  - `http://maps.googleapis.com/maps/api/geocode/json?address=`
  - `http://www.smallte.ch/applist_`
  - `http://xvo.ch/weather/`
  - `http://weatherpxauto.xvo.ch/l2g`
  - `http://i.smte.ch/istock`
- The unprotected communication of the App via http connections can be eavesdroped or maliciously modified.
  - `http://droidexp-featured.appspot.com/listappfromexo?lang=`

- `http://fonts.googleapis.com/css?family=Open+Sans:400,300,300italic,400italic,600,600italic,700,700italic,800,800italic&subset=latin,latin-ext\`
- `http://maps.googleapis.com/maps/api/geocode/json?address=`
- `http://maps.googleapis.com/maps/api/geocode/json?latlng=`
- `http://play.google.com/store/apps/details?id=com.facebook.orca`
- `http://share.weatherxl.com/?b=`
- `http://www.wunderground.com/?apiref=6b82b4478782f4bf`

Data security

- The application requires the following permissions from the protection-level: NORMAL
  - WAKE-LOCK (Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming.)
  - ACCESS-NETWORK-STATE (Allows applications to access information about networks.)
  - RECEIVE-BOOT-COMPLETED (Allows an application to receive the android.content.Intent ACTION-BOOT-COMPLETED that is broadcast after the system finishes booting. If you don't request this permission, you will not receive the broadcast at that time. Though holding this permission does not have any security implications, it can have a negative impact on the user experience by increasing the amount of time it takes the system to start and allowing applications to have themselves running without the user being aware of them. As such, you must explicitly declare your use of this facility to make that visible to the user.)
- The application requires the following permissions from the protection-level: DANGEROUS
  - ACCESS-FINE-LOCATION (Allows an app to access precise location from location sources such as GPS, cell towers, and Wi-Fi.)
  - INTERNET (Allows applications to open network sockets.)
- Application uses userdefined permissions. Application can access data of a foreign application which requires this permission to access data.

- No indicators for overprivilege/redundant permissions found! The defined permission can not abused by foreign apps.
- The application uses a content provider for interacting with data set structures. Content providers are the standard interface that connects data in one process with code running in another process.
- Every ContentProvider defined in the application is protected by a permission. To access the interface from an external application it must request access to it. The interface is only available if an application defines these permissions.
- Indicator for JavaScript bridge to Android API usage found. JavaScript used in the application (localy stored or loaded dynamicaly) may access and execute Android SDK API calls.
- Wifi-Direct is not enabled. There is no risk for exploiting a vulnerability in the wpa-supplicant module responsible for the wlan management. (http://www.coresecurity.com/advisories/android-wifi-direct-denial-service)

Input interface security

- No indicators for file handling found. The app does not define a filter scheme to process specific files.
- The app does not use protection measures for preventing screenshots. For apps displaying sensitive data it is recommended to disable screenshots.
- The application is vulnerable to tapjacking. When the protection is not used inside an exported activity another application is able to redirect touch events to the exported activity without the users consent.

Privacy

- Code obfuscation techniques were detected for the app.
- Obfuscation levels are rated as LOW, MEDIUM, ABOVE MEDIUM, HIGH or UNKNOWN. The detected obfuscation level of HIGH provides sophisticated protection against manual analysis which requires a high effort and deep knowledge to reverse the functionality of the app.
- Device administration features not used.
- Application reads out different unique device Ids. These unique identifiers allows to identify the device and to distinguish it from other devices. Another option for reading out these IDs allow to determine the environment. The application can determine if it is running on a real device or on a virtual/emulated device.

- Accessed unique identifier(s): `build model`, `build manufacturer`, `build product`, `build display`, `build fingerprint`, `build brand`, `country code + mobile network code for SIM provider`, `MMC (Mobile Country Code)`, `unique Android ID`
- Indicators for usage of advertisement/tracking framework were found.
- The application contains components (Activities) which are exported. This means these parts of the application are accessible or executable by other applications. An external app can write or read information/data to or from this app. Additionally components of this application can be executed. Following Activities are exported:
  - `com.facebook.CustomTabActivity`
  - `com.exovoid.weather.widget.WidgetFavActivity4x3`
  - `com.exovoid.weather.widget.WidgetFavActivity4x1`
  - `com.exovoid.weather.app.WallpaperSettings`
  - `com.exovoid.weather.widget.WidgetFavActivity4x2`
- In this application the allow backup option is enabled. This means the application and all application data will be included when performing a device backup. In case the application contains sensitive information these can be extracted from the backup archive or cloned onto other devices.
- Logging statements found in app. This might leak security or privacy relevant information.
- Permission READ-CONTACTS not used.
- Application reads information from different sensors. This allows the application to track the user and/or determine the environment of the user.
- World readable/writable files detected which can be read/written by other applications.
  - WORLD-READABLE
- App contains URL(s) that indicate an unprotected HTTP access to map providers. The transmitted location query parameters to the following map providers are in this case accesible by third parties:
  - Google Maps

- World readable/writable preference files detected which can be read/written by other applications.
  - WORLD-READABLE

Runtime Security

- The application contains a registered scheduled alarm. With such an alarm the application repeats the execution of the registered task for example every 10 hours. The following classes register scheduled tasks:
  - `com.exovoid.weather.app.RefreshBroadcastReceiver`
- The scheduled task gets repeated in the following intervals:
  - Dynamic interval(s)
- The alarm manager has been initialized properly.
- Indicators found for dynamic code loading. The application loads executable code during runtime from a local or external source.
- Android dalvik code is loaded dynamically by the listed methods. Native code by Java Native Interface (for dynamic loading) is used.
- In the AndroidManifest.xml file the debuggable option is disabled. This prevents some attempts for debugging the application over the adb debug bridge with jdb. Depending of the used Android operating system this flag is not mandatory, in custom ROMs or rooted devices the OS may ignore this flag. On a non stock Android ROM this can still be misused for dynamic analyzes of the application or for doing runtime manipulation. This option should be disabled in released applications.
- Loadable libraries found:
  - `ARM 32 bit: lib/armeabi-v7a/libgdx.so`
  - `ARM 32 bit: lib/armeabi/libgdx.so`
  - `x86 32bit: lib/x86/libgdx.so`
- The Application has the permission to start automatically after booting the device. The application can execute code without userinteraction or prevention.

Test Performance

- Execution time of all tests: 0:01:08.650

3.14 Wetter Live Kostenlos (Android)

3.14.1 Tests

The following Table 3.15 summarizes the results of the Android app `Wetter Live Kostenlos` with version *5.1*.

Table 3.15: Overview of summarized test results for »Wetter Live Kostenlos«

App risks for enterprise usage	
☒	*Implementation flaws? Yes.*
☒	*Privacy risks? Yes.*
☒	*Security risks? Yes.*
Blacklisted by policy	
☐	*Violations of default policy? No.*
Communication security	
☒	*Client communication used? Yes.*
☑	*Communication endpoints: 53 entries, see details.*
☑	*Communication with country: 7 entries, see details.*
☒	*SSL/TLS used? Yes.*
☑	*Domains accessed with http AND https:* `play.google.com`
☒	*Custom SSL/TLS trust manager implemented? Yes.*
☒	*Faulty custom SSL/TLS trust manager implemented? Yes.*
☒	*SSL/TLS using custom error handling? Yes.*
☐	*SSL/TLS using faulty custom error handling? No.*
☒	*SSL/TLS using manual domain name verification? Yes.*
☒	*Unprotected HTML? Yes.*
☒	*Unprotected communication? Yes.*
Data security	
☑	*Cryptographic Primitives:* `"AES/CBC/PKCS5Padding", "AES/ECB/PKCS5Padding", "AES/ECB/PKCS7Padding"`
☒	*Application needs normal permissions? Yes.*
☒	*Application needs dangerous permissions? Yes.*
☑	*Userdefined permission usage: 6 entries, see details.*
☑	*Overprivileged permissions:* `READ-PHONE-STATE`
☒	*Is application overprivileged? Yes.*
☒	*Application defines content provider? Yes.*
−	*Content provider accessible without permission: None.*
☒	*JavaScript to SDK API bridge usage? Yes.*
☐	*WiFi-Direct enabled? No.*
Input interface security	
−	*App can handle documents of mimeType: None.*
☐	*Screenshot protection used? No.*

☐	*Tap Jacking Protection used? No.*
Privacy	
☒	*Obfuscation used? Yes.*
☑	*Obfuscation level is:* `HIGH`
−	*Device administration policy entries: None.*
☑	*Accessed unique identifier(s): 10 entries, see details.*
☑	*Advertisment-/tracking frameworks found: 6 entries, see details.*
☒	*App provides public accessible activities? Yes.*
☒	*Backup of app is allowed? Yes.*
☒	*Log Statement Enabled? Yes.*
☐	*Permission to access address book? No.*
☑	*Sensor usage:* `WIFI-Based Location`, `GPS Location`
☒	*Unprotected preference files found? Yes.*
Runtime Security	
☒	*Scheduled Alarm Manager registered? Yes.*
☑	*Alarm repeating types:* `RTC`, `ELAPSED-REALTIME`
☒	*Alarm intervals dynamically? Yes.*
☐	*Alarm Manager initialized dynamically? No.*
☒	*Dynamically loaded code at runtime? Yes.*
☑	*Dynamically loaded code at runtime type(s):* `dalvik.system.DexClassLoader(...)`, `dalvik.system.PathClassLoader(...)`, `ClassLoader.loadClass(...)`
☐	*Allow app debugging Flag? No.*
☑	*Executed component after Phone Reboot:* `com.apalon.weatherlive.remote.WeatherDataUpdateReceiver`

3.14.2 Details

The following sections describe details about the test results of `Wetter Live Kostenlos` with version *5.1*.

App risks for enterprise usage

- Reasons for category implementation flaws:
  - Possible flaw: App contains insecure code for communication protection with SSL/TLS. Common source for flawed communication protection against man-in-the-middle attacks.
  - Possible flaw: unintended use of insecure HTTP protocol for transmissions of parameters to servers capable of HTTPS.
- Reasons for category privacy risks:

  - Advertisement/Tracking: App uses more than 5 advertisement and tracking providers.

- Reasons for category security risks:

  - Unprotected Web Content: App loads active web content (e.g. JavaScript or HTML files) without integrity protection. This poses a risk as man-in-the-middle attackers can modify the loaded web content and change the functionality of the app.

Communication security

- Client communication detected. The application can establish a network connection to one or more specific host systems. URLs with parameters found:

  - `amzn://apps/android?p=`
  - `flurry://flurrycall?event=`
  - `flurry://flurrycall?event=adWillClose`
  - `http://api.accuweather.com/locations/v1/%s.json?apikey=eef88a8fb2cb407a9fbd2ebdf138d7e6&language=%s&details=false`
  - `http://api.accuweather.com/locations/v1/cities/autocomplete.json?q=%s&apikey=eef88a8fb2cb407a9fbd2ebdf138d7e6&language=%s`
  - `http://api.accuweather.com/locations/v1/cities/geoposition/search.json?q=%s,%s&apikey=eef88a8fb2cb407a9fbd2ebdf138d7e6&language=%s&details=false`
  - `http://api.accuweather.com/locations/v1/postalcodes/search.json?q=%s&apikey=eef88a8fb2cb407a9fbd2ebdf138d7e6&language=%s`
  - `http://feed.foreca.com/apalon-feb14/search.php?q=%s&lang=%s`
  - `http://play.google.com/store/apps/details?id=com.facebook.orca`
  - `http://report.weatherlive.info/android/api/confirmReport?data=%s`
  - `http://report.weatherlive.info/android/api/notIdenticalLocations?data=`

- http://report.weatherlive.info/android/api/notIdenticalLocations?data=%s
- http://report.weatherlive.info/android/api/v1/setWeatherState?data=%s
- http://weatherlive.info/location_weather.php?q=%s&language=%s
- http://www.shutterstock.com/pic.mhtml?id=101532181&src=id
- http://www.shutterstock.com/pic.mhtml?id=137820215&src=id
- http://www.shutterstock.com/pic.mhtml?id=141803128&src=id
- http://www.shutterstock.com/pic.mhtml?id=151664060&src=id
- http://www.shutterstock.com/pic.mhtml?id=164630048&src=id
- http://www.shutterstock.com/pic.mhtml?id=55606732&src=id
- http://www.shutterstock.com/pic.mhtml?id=64391617&src=id
- http://www.shutterstock.com/pic.mhtml?id=70237327&src=id
- http://www.shutterstock.com/pic.mhtml?id=78457405&src=id
- http://www.shutterstock.com/pic.mhtml?id=83071804&src=id
- http://www.shutterstock.com/pic.mhtml?id=85539823&src=id
- https://app.adjust.io/%s?campaign=%s&tracker_limit=100000
- https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps
- https://play.google.com/store/apps/details?id=
- https://play.google.com/store/apps/details?id=com.apalon.weatherlive.free

  - `https://www.tumblr.com/oauth/authorize?oauth_token=%s`
  - `market://details?id=`
  - `market://details?id=%s`
  - `market://details?id=com.facebook.orca`
  - `market://details?id=com.google.android.gms.ads`

- Communication endpoints is a list of all potential communication endpoints Appicaptor was able to detect. This allows quick enumeration of suspicious domains, raw IP Addresses, etc..
- Communication endpoints: `.facebook.com`, `adlog.flurry.com`, `ads.flurry.com`, `amazon-adsystem.com`, `apalon.com`, `api.accuweather.com`, `api.pubnative.net`, `api.tumblr.com`, `app-measurement.com`, `app.adjust.com`, `app.adjust.io`, `appsettings.apalon.com`, `cdn.flurry.com`, `csi.gstatic.com`, `data.flurry.com`, `denisftpu.herewetest.com`, `dwxjayoxbnyrr.cloudfront.net`, `e.crashlytics.com`, `exchangerates.herewetest.com`, `facebook.com`, `feed.foreca.com`, `freegeoip.net`, `geoip.weatherlive.info`, `github.com`, `gma.foreca.com`, `googleads.g.doubleclick.net`, `graph-video.%s`, `graph.%s`, `graph.%s.facebook.com`, `graph.facebook.com`, `io.appmessages.com`, `m.facebook.com`, `mads.amazon-adsystem.com`, `pagead2.googlesyndication.com`, `play.google.com`, `plus.google.com`, `project.herewetest.com`, `proton.flurry.com`, `report.weatherlive.info`, `settings.crashlytics.com`, `twitter.com`, `weather.herewetest.com`, `weatherkindle.herewetest.com`, `weatherlive.info`, `weatherlivefree.herewetest.com`, `www.%s.facebook.com`, `www.apalon.com`, `www.facebook.com`, `www.google.com`, `www.googleapis.com`, `www.shutterstock.com`, `www.timeapi.org`, `www.tumblr.com`
- App communicates with servers in 7 countries.
- Communication with country: `Canada`, `United States`, `Ireland`, `Finland`, `United Kingdom`, `Germany`, `unknown`
- Usage of SSL/TLS can protect the App's communication from adversaries. Tests indicate that communication is at least partly protected with SSL/TLS.

- Mixed usage of HTTP and HTTPS: Protected and unprotected submission of parameters to the same domain. Indicates implementation flaw or weak communication protection.
- Modifications of trust management found. Interface X509TrustManager is implemented or extended.
- The SSL trust management for socket communication is modified in an insecure way. The following implementations of the X509TrustManager interface should be checked:
  - `Lcom/apalon/helpmorelib/badge/ConfigLoader$1.`
- Modifications of the SSL error handling detected: Class WebViewClient is extended and onReceivedSslError(...) is overwritten.
- Correct verification of the corresponding client hostname is important for SSL/TLS security. The app changes the secure default hostname verification by the following:
  - Interface HostnameVerifier is implemented or extended.
- The app loads the following HTML files via unprotected communication (http), which can be exploited by attackers to remotely change the displayed content and functionality of the app:
  - `http://weatherlive.info/android/api/`
  - `http://report.weatherlive.info/android/api/confirmReport?data=%s`
  - `http://geoip.weatherlive.info/myip`
  - `http://weather.herewetest.com/utc_now.php`
  - `http://apalon.com/wl`
  - `http://www.timeapi.org/utc/now`
  - `http://weatherlive.info/api/v1/feed`
  - `http://project.herewetest.com/weather_live_gp_full_v_3_2/help_`
  - `http://report.weatherlive.info/android/api/notIdenticalLocations?data=`
  - `http://report.weatherlive.info/android/api/report`
  - `http://report.weatherlive.info/android/api/v1/setWeatherState?data=%s`

  - http://project.herewetest.com/weather_live_free_gp_2_2/help_
  - http://project.herewetest.com/weather_live_free_amazon_3_1/help_
  - http://weatherlive.info/api/location
  - http://apalon.com/f_wl
  - http://project.herewetest.com/weather_live_amazon_3_8/help_
  - http://project.herewetest.com/weather_live_amazon_3_1/help_
  - http://exchangerates.herewetest.com/exchange/
  - http://www.tumblr.com/connect/login_success.html
  - http://api.pubnative.net/api/v3/native
  - http://feed.foreca.com/apalon-feb14/search.php?q=%s&lang=%s
  - http://weatherlive.info/location_weather.php?q=%s&language=%s
  - http://www.apalon.com/terms_of_use.html
  - http://m.facebook.com/ads/ad_choices
  - http://freegeoip.net/json/
  - http://www.apalon.com/privacy_policy.html
  - http://report.weatherlive.info/android/api/notIdenticalLocations?data=%s

- The unprotected communication of the App via http connections can be eavesdroped or maliciously modified.
  - http://api.accuweather.com/locations/v1/%s.json?apikey=eef88a8fb2cb407a9fbd2ebdf138d7e6&language=%s&details=false
  - http://api.accuweather.com/locations/v1/cities/autocomplete.json?q=%s&apikey=eef88a8fb2cb407a9fbd2ebdf138d7e6&language=%s

- http://api.accuweather.com/locations/v1/cities/geoposition/search.json?q=%s,%s&apikey=eef88a8fb2cb407a9fbd2ebdf138d7e6&language=%s&details=false
- http://api.accuweather.com/locations/v1/postalcodes/search.json?q=%s&apikey=eef88a8fb2cb407a9fbd2ebdf138d7e6&language=%s
- http://feed.foreca.com/apalon-feb14/search.php?q=%s&lang=%s
- http://play.google.com/store/apps/details?id=com.facebook.orca
- http://report.weatherlive.info/android/api/confirmReport?data=%s
- http://report.weatherlive.info/android/api/notIdenticalLocations?data=
- http://report.weatherlive.info/android/api/notIdenticalLocations?data=%s
- http://report.weatherlive.info/android/api/v1/setWeatherState?data=%s
- http://weatherlive.info/location_weather.php?q=%s&language=%s
- http://www.shutterstock.com/pic.mhtml?id=101532181&src=id
- http://www.shutterstock.com/pic.mhtml?id=137820215&src=id
- http://www.shutterstock.com/pic.mhtml?id=141803128&src=id
- http://www.shutterstock.com/pic.mhtml?id=151664060&src=id
- http://www.shutterstock.com/pic.mhtml?id=164630048&src=id
- http://www.shutterstock.com/pic.mhtml?id=55606732&src=id
- http://www.shutterstock.com/pic.mhtml?id=64391617&src=id
- http://www.shutterstock.com/pic.mhtml?id=70237327&src=id

- http://www.shutterstock.com/pic.mhtml?id=78457405&src=id
- http://www.shutterstock.com/pic.mhtml?id=83071804&src=id
- http://www.shutterstock.com/pic.mhtml?id=85539823&src=id

Data security

- ECB mode usage identified. This mode has the disadvantage, that identical plaintext blocks are encrypted into identical ciphertext blocks. Therefore it does not hide patterns well and this mode is not recommended for use in cryptographic protocols at all.
- The application requires the following permissions from the protection-level: NORMAL
  - RECEIVE-BOOT-COMPLETED (Allows an application to receive the android.content.Intent ACTION-BOOT-COMPLETED that is broadcast after the system finishes booting. If you don't request this permission, you will not receive the broadcast at that time. Though holding this permission does not have any security implications, it can have a negative impact on the user experience by increasing the amount of time it takes the system to start and allowing applications to have themselves running without the user being aware of them. As such, you must explicitly declare your use of this facility to make that visible to the user.)
  - ACCESS-NETWORK-STATE (Allows applications to access information about networks.)
  - WAKE-LOCK (Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming.)
- The application requires the following permissions from the protection-level: DANGEROUS
  - ACCESS-COARSE-LOCATION (Allows an app to access approximate location derived from network location sources such as cell towers and Wi-Fi.)
  - INTERNET (Allows applications to open network sockets.)
  - ACCESS-FINE-LOCATION (Allows an app to access precise location from location sources such as GPS, cell towers, and Wi-Fi.)
  - READ-PHONE-STATE (Allows read only access to phone state. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)

- Application uses userdefined permissions. Application can access data of a foreign application which requires this permission to access data.
- Userdefined permission usage: `com.apalon.weatherlive.free.permission.C2D-MESSAGE`, `com.samsung.android.providers.context.permission.WRITE-USE-APP-FEATURE-SURVEY`, `com.android.vending.BILLING`, `com.google.android.permission.PROVIDE-BACKGROUND`, `com.google.android.c2dm.permission.RECEIVE`, `com.google.android.providers.gsf.permission.READ-GSERVICES`
- Application is propably overprivileged. Application has too much permissions. Foreign applications may be able to abuse this permission.
- The application uses a content provider for interacting with data set structures. Content providers are the standard interface that connects data in one process with code running in another process.
- Every ContentProvider defined in the application is protected by a permission. To access the interface from an external application it must request access to it. The interface is only available if an application defines these permissions.
- Indicator for JavaScript bridge to Android API usage found. JavaScript used in the application (localy stored or loaded dynamicaly) may access and execute Android SDK API calls.
- Wifi-Direct is not enabled. There is no risk for exploiting a vulnerability in the wpa-supplicant module responsible for the wlan management. (http://www.coresecurity.com/advisories/android-wifi-direct-denial-service)

Input interface security

- No indicators for file handling found. The app does not define a filter scheme to process specific files.
- The app does not use protection measures for preventing screenshots. For apps displaying sensitive data it is recommended to disable screenshots.
- The application is vulnerable to tapjacking. When the protection is not used inside an exported activity another application is able to redirect touch events to the exported activity without the users consent.

Privacy

- Code obfuscation techniques were detected for the app.

- Obfuscation levels are rated as LOW, MEDIUM, ABOVE MEDIUM, HIGH or UNKNOWN. The detected obfuscation level of HIGH provides sophisticated protection against manual analysis which requires a high effort and deep knowledge to reverse the functionality of the app.
- Device administration features not used.
- Application reads out different unique device Ids. These unique identifiers allows to identify the device and to distinguish it from other devices. Another option for reading out these IDs allow to determine the environment. The application can determine if it is running on a real device or on a virtual/emulated device.
- Accessed unique identifier(s): `build model`, `build manufacturer`, `build product`, `build display`, `build fingerprint`, `build brand`, `Wifi-MAC address`, `country code + mobile network code for SIM provider`, `MMC (Mobile Country Code)`, `unique Android ID`
- Indicators for usage of advertisement/tracking framework were found.
- Advertisment-/tracking frameworks found: `Adjust`, `Amazon Ad System`, `Crashlytics`, `Doubleclick`, `Flurry`, `inMobi ADs`
- The application contains components (Activities) which are exported. This means these parts of the application are accessible or executable by other applications. An external app can write or read information/data to or from this app. Additionally components of this application can be executed. Following Activities are exported:
  - `com.apalon.weatherlive.widget.weather.ActivityWeatherWidgetConfiguration`
- In this application the allow backup option is enabled. This means the application and all application data will be included when performing a device backup. In case the application contains sensitive information these can be extracted from the backup archive or cloned onto other devices.
- Logging statements found in app. This might leak security or privacy relevant information.
- Permission READ-CONTACTS not used.
- Application reads information from different sensors. This allows the application to track the user and/or determine the environment of the user.
- World readable/writable preference files detected which can be read/written by other applications.
  - WORLD-READABLE

Runtime Security

- The application contains a registered scheduled alarm. With such an alarm the application repeats the execution of the registered task for example every 10 hours. The following classes register scheduled tasks:
  - `com.apalon.weatherlive.widget.weather.b`
  - `com.apalon.weatherlive.i.c`
- The scheduled task gets repeated in the following intervals:
  - Dynamic interval(s)
- The alarm manager has been initialized properly.
- Indicators found for dynamic code loading. The application loads executable code during runtime from a local or external source.
- Android dalvik code is loaded dynamically by the listed methods.
- In the AndroidManifest.xml file the debuggable option is disabled. This prevents some attempts for debugging the application over the adb debug bridge with jdb. Depending of the used Android operating system this flag is not mandatory, in custom ROMs or rooted devices the OS may ignore this flag. On a non stock Android ROM this can still be misused for dynamic analyzes of the application or for doing runtime manipulation. This option should be disabled in released applications.
- The Application has the permission to start automatically after booting the device. The application can execute code without userinteraction or prevention.

Test Performance

- Execution time of all tests: 0:01:09.687

3.15 Wetter Radar Schnee MORECAST. (Android)

3.15.1 Tests

The following Table 3.16 summarizes the results of the Android app `Wetter Radar Schnee MORECAST.` with version *3.1.2*.

Table 3.16: Overview of summarized test results for »Wetter Radar Schnee MORECAST.«

App risks for enterprise usage	
☐	*Implementation flaws? No.*
☒	*Privacy risks? Yes.*
☒	*Security risks? Yes.*

Blacklisted by policy

☐ *Violations of default policy? No.*

Communication security

☒ *Client communication used? Yes.*
☑ *Communication endpoints: 45 entries, see details.*
☑ *Communication with country: 6 entries, see details.*
☒ *SSL/TLS used? Yes.*
☐ *Custom SSL/TLS trust manager implemented? No.*
☒ *SSL/TLS using custom error handling? Yes.*
☐ *SSL/TLS using faulty custom error handling? No.*
☐ *SSL/TLS using manual domain name verification? No.*
☒ *Unprotected HTML? Yes.*
☒ *Unprotected JavaScripts? Yes.*
☒ *Unprotected communication? Yes.*

Data security

☑ *Cryptographic Primitives:* `"AES/CBC/PKCS5Padding"`, `"PBEWithMD5AndDES"`
☑ *Key derivation iteration count:* `20`
☒ *Application needs normal permissions? Yes.*
☒ *Application needs dangerous permissions? Yes.*
☑ *Userdefined permission usage:* `android.permission.WRITE_INTERNAL_STORAGE`, `com.ubimet.morecast.permission.C2D_MESSAGE`, `com.google.android.c2dm.permission.RECEIVE`
☐ *Is application overprivileged? No.*
☒ *Application defines content provider? Yes.*
⊟ *Content provider accessible without permission: None.*
☒ *JavaScript to SDK API bridge usage? Yes.*
☐ *WiFi-Direct enabled? No.*

Input interface security

⊟ *App can handle documents of mimeType: None.*
☐ *Screenshot protection used? No.*
☐ *Tap Jacking Protection used? No.*

Privacy

☒ *Obfuscation used? Yes.*
☑ *Obfuscation level is:* `UNKNOWN`
⊟ *Device administration policy entries: None.*
☑ *Accessed unique identifier(s): 11 entries, see details.*
☑ *Advertisment-/tracking frameworks found:* `Crashlytics`, `Doubleclick`, `Smaato`
☒ *App provides public accessible activities? Yes.*
☒ *Backup of app is allowed? Yes.*

☒	*Log Statement Enabled? Yes.*
☐	*Permission to access address book? No.*
☑	*Sensor usage:* `WIFI-Based Location`, `GPS Location`
☒	*Unprotected map queries? Yes.*
☒	*Unprotected preference files found? Yes.*

Runtime Security

☒	*Scheduled Alarm Manager registered? Yes.*
☑	*Alarm repeating types:* `ELAPSED-REALTIME`
☒	*Alarm intervals dynamically? Yes.*
☐	*Alarm Manager initialized dynamically? No.*
☒	*Dynamically loaded code at runtime? Yes.*
☑	*Dynamically loaded code at runtime type(s):* `dalvik.system.DexClassLoader(...)`, `ClassLoader.loadClass(...)`, `loadLibrary(...)`
☐	*Allow app debugging Flag? No.*
☒	*Contains native libraries: Yes.*
☑	*Executed component after Phone Reboot:* `com.ubimet.morecast.common.scheduling.AutoStartAtBoot`

3.15.2 Details

The following sections describe details about the test results of `Wetter Radar Schnee MORECAST.` with version *3.1.2*.

App risks for enterprise usage

- Reasons for category privacy risks:
  - App tries to access the device phone number which can be use to identify the owner remotely.
  - Unprotected Access: Disclosure of location or web query data though unprotected communication with service providers.
- Reasons for category security risks:
  - Unprotected Web Content: App loads active web content (e.g. JavaScript or HTML files) without integrity protection. This poses a risk as man-in-the-middle attackers can modify the loaded web content and change the functionality of the app.

Communication security

- Client communication detected. The application can establish a network connection to one or more specific host systems. URLs with parameters found:

  - `http://dev.virtualearth.net/REST/V1/Imagery/Metadata/%s?mapVersion=v1&output=json&key=%s`
  - `http://play.google.com/store/apps/details?id=com.facebook.orca`
  - `http://www.facebook.com/sharer/sharer.php?u=https://app.adjust.com/yrpndw`
  - `https://a.tiles.mapbox.com/v4/%s.json?access_token=%s&secure=1`
  - `https://a.tiles.mapbox.com/v4/%s.json?secure&access_token=%s`
  - `https://a.tiles.mapbox.com/v4/%s/%s?access_token=%s`
  - `https://docs.google.com/gview?embedded=true&url=`
  - `https://docs.google.com/gview?embedded=true&url=http://morecast.com/content/uploads/2015/07/DE.pdf`
  - `https://docs.google.com/gview?embedded=true&url=http://morecast.com/content/uploads/2015/07/EN.pdf`
  - `https://docs.google.com/gview?embedded=true&url=http://morecast.com/content/uploads/2015/07/US.pdf`
  - `https://docs.google.com/gview?embedded=true&url=http://morecast.com/content/uploads/2015/10/AU.pdf`
  - `https://maps.googleapis.com/maps/api/geocode/json?latlng=`
  - `https://twitter.com/intent/tweet?text=`
  - `https://www.googleapis.com/oauth2/v1/userinfo?alt=json`
  - `market://details?id=com.facebook.orca`
  - `market://details?id=com.google.android.gms.ads`

- Communication endpoints is a list of all potential communication endpoints Appicaptor was able to detect. This allows quick enumeration of suspicious domains, raw IP Addresses, etc..

- Communication endpoints: .facebook.com, a.tiles.mapbox.com, accounts.google.com, admin.appnext.com, api-eu.morecast.com, api-fhdemo.morecast.com, api-us-dev.morecast.com, api-us.morecast.com, api.morecast.com, app-measurement.com, app.adjust.com, app.getsentry.com, avr.smaato.net, csi.gstatic.com, d3skaoddt9qiqw.cloudfront.net, dev.virtualearth.net, docs.google.com, facebook.com, googleads.g.doubleclick.net, graph-video.%s, graph.%s, graph.accountkit.com, here.com, login.live.com, login.yahoo.com, m.facebook.com, maps.googleapis.com, morecast.com, play.google.com, plus.google.com, s3.eu-central-1.amazonaws.com, smaato-android-sdk.s3.amazonaws.com, soma-assets.smaato.net, soma.smaato.net, ssl.google-analytics.com, twitter.com, www.accountkit.com, www.bom.gov.au, www.facebook.com, www.google-analytics.com, www.google.com, www.googleapis.com, www.googletagmanager.com, www.linkedin.com, www.paypal.com
- App communicates with servers in 6 countries.
- Communication with country: Austria, United States, Ireland, Australia, Germany, unknown
- Usage of SSL/TLS can protect the App's communication from adversaries. Tests indicate that communication is at least partly protected with SSL/TLS.
- App uses the secure default SSL/TLS implementation for client communication. Error-prone modifications were not detected.
- Modifications of the SSL error handling detected: Class WebViewClient is extended and onReceivedSslError(...) is overwritten.
- The app loads the following HTML files via unprotected communication (http), which can be exploited by attackers to remotely change the displayed content and functionality of the app:
  - http://www.facebook.com/sharer/sharer.php?u=https://app.adjust.com/yrpndw
  - http://avr.smaato.net/report
  - http://dev.virtualearth.net/REST/V1/Imagery/Metadata/%s?mapVersion=v1&output=json&key=%s
  - http://here.com/terms
  - http://admin.appnext.com/AdminService.asmx/ery

  - `http://soma.smaato.net/oapi/reqAd.jsp?`

- The app loads the following JavaScript files via unprotected communication (http), which can be exploited by attackers to remotely change the displayed content and functionality of the app:
  - `http://soma-assets.smaato.net/js/ormma.js`
  - `http://soma-assets.smaato.net/js/ormma_bridge.js`
- The unprotected communication of the App via http connections can be eavesdroped or maliciously modified.
  - `http://dev.virtualearth.net/REST/V1/Imagery/Metadata/%s?mapVersion=v1&output=json&key=%s`
  - `http://play.google.com/store/apps/details?id=com.facebook.orca`
  - `http://www.facebook.com/sharer/sharer.php?u=https://app.adjust.com/yrpndw`

Data security

- Key derivation functions with less than 1000 interations are considered vulnerable to bruteforce attacks. Therefore, this app with 20 iterations is considered vulnerable.
- The application requires the following permissions from the protection-level: NORMAL
  - GET-ACCOUNTS (Allows access to the list of accounts in the Accounts Service.)
  - READ-EXTERNAL-STORAGE (Allows an application to read from external storage. Any app that declares the WRITE-EXTERNAL-STORAGE permission is implicitly granted this permission. Currently, this permission is not enforced and all apps still have access to read from external storage without this permission. That will change in a future release and apps will require this permission to read from external storage. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
  - ACCESS-NETWORK-STATE (Allows applications to access information about networks.)
  - WAKE-LOCK (Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming.)

  - RECEIVE-BOOT-COMPLETED (Allows an application to receive the android.content.Intent ACTION-BOOT-COMPLETED that is broadcast after the system finishes booting. If you don't request this permission, you will not receive the broadcast at that time. Though holding this permission does not have any security implications, it can have a negative impact on the user experience by increasing the amount of time it takes the system to start and allowing applications to have themselves running without the user being aware of them. As such, you must explicitly declare your use of this facility to make that visible to the user.)
  - ACCESS-WIFI-STATE (Allows applications to access information about Wi-Fi networks)

- The application requires the following permissions from the protection-level: DANGEROUS
  - WRITE-EXTERNAL-STORAGE (Allows an application to write to external storage. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
  - READ-PHONE-STATE (Allows read only access to phone state. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
  - ACCESS-FINE-LOCATION (Allows an app to access precise location from location sources such as GPS, cell towers, and Wi-Fi.)
  - INTERNET (Allows applications to open network sockets.)
  - ACCESS-COARSE-LOCATION (Allows an app to access approximate location derived from network location sources such as cell towers and Wi-Fi.)
  - MANAGE-ACCOUNTS (Allows an application to manage the list of accounts in the AccountManager.)
- Application uses userdefined permissions. Application can access data of a foreign application which requires this permission to access data.
- No indicators for overprivilege/redundant permissions found! The defined permission can not abused by foreign apps.
- The application uses a content provider for interacting with data set structures. Content providers are the standard interface that connects data in one process with code running in another process.
- Every ContentProvider defined in the application is protected by a permission. To access the interface from an external application it must request access to it. The interface is only available if an application defines these permissions.

- Indicator for JavaScript bridge to Android API usage found. JavaScript used in the application (localy stored or loaded dynamicaly) may access and execute Android SDK API calls.
- Wifi-Direct is not enabled. There is no risk for exploiting a vulnerability in the wpa-supplicant module responsible for the wlan management. (http://www.coresecurity.com/advisories/android-wifi-direct-denial-service)

Input interface security

- No indicators for file handling found. The app does not define a filter scheme to process specific files.
- The app does not use protection measures for preventing screenshots. For apps displaying sensitive data it is recommended to disable screenshots.
- The application is vulnerable to tapjacking. When the protection is not used inside an exported activity another application is able to redirect touch events to the exported activity without the users consent.

Privacy

- Code obfuscation techniques were detected for the app.
- The obfuscation level UNKNOWN means that the application has the capability to dynamically load code from outside, which currently is not part of the analysis. Therefore, the obfuscation strength is not evaluated.
- Device administration features not used.
- Application reads out different unique device Ids. These unique identifiers allows to identify the device and to distinguish it from other devices. Another option for reading out these IDs allow to determine the environment. The application can determine if it is running on a real device or on a virtual/emulated device.
- Accessed unique identifier(s): `build model`, `build manufacturer`, `build product`, `build display`, `build fingerprint`, `build brand`, `IMEI/MEID`, `phone number`, `Wifi-MAC address`, `MMC (Mobile Country Code)`, `unique Android ID`
- Indicators for usage of advertisement/tracking framework were found.
- The application contains components (Activities) which are exported. This means these parts of the application are accessible or executable by other applications. An external app can write or read information/data to or from this app. Additionally components of this application can be executed. Following Activities are exported:

  - com.facebook.accountkit.ui.AccountKitEmailRedirectActivity
  - com.ubimet.morecast.ui.activity.SocialNetworkHelperActivity
  - com.ubimet.morecast.appwidget.MorecastAppWidgetConfigureActivity
  - com.facebook.CustomTabActivity
  - com.ubimet.morecast.ui.activity.DeepLinkActivity

- In this application the allow backup option is enabled. This means the application and all application data will be included when performing a device backup. In case the application contains sensitive information these can be extracted from the backup archive or cloned onto other devices.
- Logging statements found in app. This might leak security or privacy relevant information.
- Permission READ-CONTACTS not used.
- Application reads information from different sensors. This allows the application to track the user and/or determine the environment of the user.
- App contains URL(s) that indicate an unprotected HTTP access to map providers. The transmitted location query parameters to the following map providers are in this case accesible by third parties:
  - Microsoft Bing Maps
- World readable/writable preference files detected which can be read/written by other applications.
  - WORLD-READABLE

Runtime Security

- The application contains a registered scheduled alarm. With such an alarm the application repeats the execution of the registered task for example every 10 hours. The following classes register scheduled tasks:
  - com.ubimet.morecast.common.scheduling.AutomatedTaskManager
- The scheduled task gets repeated in the following intervals:
  - Dynamic interval(s)
- The alarm manager has been initialized properly.

- Indicators found for dynamic code loading. The application loads executable code during runtime from a local or external source.
- Android dalvik code is loaded dynamically by the listed methods. Native code by Java Native Interface (for dynamic loading) is used.
- In the AndroidManifest.xml file the debuggable option is disabled. This prevents some attempts for debugging the application over the adb debug bridge with jdb. Depending of the used Android operating system this flag is not mandatory, in custom ROMs or rooted devices the OS may ignore this flag. On a non stock Android ROM this can still be misused for dynamic analyzes of the application or for doing runtime manipulation. This option should be disabled in released applications.
- Loadable libraries found:
  - `MIPS I: lib/mips/libMaply.so`
  - `MIPS I: lib/mips/libgnustl_shared.so`
  - `MIPS I: lib/mips/libRSSupport.so`
  - `MIPS I: lib/mips/librs.blur.so`
  - `MIPS I: lib/mips/librsjni.so`
  - `x86 32bit: lib/x86/libMaply.so`
  - `x86 32bit: lib/x86/libgnustl_shared.so`
  - `x86 32bit: lib/x86/libRSSupport.so`
  - `x86 32bit: lib/x86/librs.blur.so`
  - `x86 32bit: lib/x86/librsjni.so`
  - `ARM 32 bit: lib/armeabi-v7a/libMaply.so`
  - `ARM 32 bit: lib/armeabi-v7a/libgnustl_shared.so`
  - `ARM 32 bit: lib/armeabi-v7a/libRSSupport.so`
  - `ARM 32 bit: lib/armeabi-v7a/librs.blur.so`
  - `ARM 32 bit: lib/armeabi-v7a/librsjni.so`
  - `ARM 32 bit: lib/armeabi/libMaply.so`
  - `ARM 32 bit: lib/armeabi/libgnustl_shared.so`
- The Application has the permission to start automatically after booting the device. The application can execute code without userinteraction or prevention.

Test Performance

- Execution time of all tests: 0:01:13.429

3.16 Wetter und Radar - wetter.com (Android)

3.16.1 Tests

The following Table 3.17 summarizes the results of the Android app `Wetter und Radar – wetter.com` with version *2.12.3*.

Table 3.17: Overview of summarized test results for »Wetter und Radar - wetter.com«

App risks for enterprise usage	
☒	*Implementation flaws? Yes.*
☒	*Privacy risks? Yes.*
☒	*Security risks? Yes.*
Blacklisted by policy	
☒	*Violations of default policy? Yes.*
Communication security	
☒	*Client communication used? Yes.*
☑	*Communication endpoints: 63 entries, see details.*
☑	*Communication with country: 8 entries, see details.*
☒	*SSL/TLS used? Yes.*
☑	*Domains accessed with http AND https:* `play.google.com`
☐	*Custom SSL/TLS trust manager implemented? No.*
☒	*SSL/TLS using custom error handling? Yes.*
☐	*SSL/TLS using faulty custom error handling? No.*
☐	*SSL/TLS using manual domain name verification? No.*
☒	*Unprotected HTML? Yes.*
☒	*Unprotected JavaScripts? Yes.*
☒	*Unprotected communication? Yes.*
Data security	
☑	*Cryptographic Primitives:* `"AES/CBC/PKCS7Padding"`, `"AES/ECB/PKCS7Padding"`, `"RSA/NONE/NoPadding"`
☒	*Cryptographic keys found? Yes.*
☒	*Application needs normal permissions? Yes.*
☒	*Application needs dangerous permissions? Yes.*
☑	*Userdefined permission usage:* `com.android.vending.BILLING`, `com.google.android.c2dm.permission.RECEIVE`
☐	*Is application overprivileged? No.*
☒	*Application defines content provider? Yes.*
⊟	*Content provider accessible without permission: None.*

☒ *JavaScript to SDK API bridge usage? Yes.*
☐ *WiFi-Direct enabled? No.*

Input interface security

☒ *App can handle documents of mimeType: None.*
☐ *Screenshot protection used? No.*
☐ *Tap Jacking Protection used? No.*

Privacy

☒ *Installed app list accessed? Yes.*
☒ *Obfuscation used? Yes.*
☑ *Obfuscation level is:* `HIGH`
☒ *Device administration policy entries: None.*
☑ *Accessed unique identifier(s): 10 entries, see details.*
☑ *Advertisment-/tracking frameworks found: 8 entries, see details.*
☐ *App provides public accessible activities? No.*
☒ *Backup of app is allowed? Yes.*
☒ *Log Statement Enabled? Yes.*
☐ *Permission to access address book? No.*
☑ *Sensor usage:* `Camera (inactive)`, `WIFI-Based Location`, `GPS Location`, `Acceleration/Light`
☒ *Unprotected preference files found? Yes.*

Runtime Security

☐ *Scheduled Alarm Manager registered? No.*
☒ *Dynamically loaded code at runtime? Yes.*
☑ *Dynamically loaded code at runtime type(s):* `ClassLoader.loadClass(...)`
☐ *Allow app debugging Flag? No.*
☒ *App uses outdated signature key? Yes.*
☒ *Contains native libraries: Yes.*
☑ *Executed component after Phone Reboot:* `com.wetter.androidclient.notifications.alarm.OnBootReceiver`

3.16.2 Details

The following sections describe details about the test results of `Wetter und Radar - wetter.com` with version *2.12.3*.

App risks for enterprise usage

- Reasons for category implementation flaws:
  - Possible flaw: unintended use of insecure HTTP protocol for transmissions of parameters to servers capable of HTTPS.

- Reasons for category privacy risks:
  - Advertisement/Tracking: App uses more than 5 advertisement and tracking providers.
  - App Listing: Usage of detected functionality to access list of installed apps poses a privacy risk for detected app type.
- Reasons for category security risks:
  - Unprotected Web Content: App loads active web content (e.g. JavaScript or HTML files) without integrity protection. This poses a risk as man-in-the-middle attackers can modify the loaded web content and change the functionality of the app.
  - Crypto: Embedded static encryption key found, which can be extracted by attackers to revert the encryption or fake the signature of the content it is used for.

Blacklisted by policy

- Reasons for category violations of default policy:
  - Estimated overall app risk for the enterprise exceeds the security policy threshold due to detected risks and flaws exploitable by skilled attackers without the existence of additional supporting factors.

Communication security

- Client communication detected. The application can establish a network connection to one or more specific host systems. URLs with parameters found:
  - `amzn://apps/android?p=`
  - `flurry://flurrycall?event=`
  - `flurry://flurrycall?event=adWillClose`
  - `http://1.aerial.maps.api.here.com//maptile/2.1/maptile/newest/%1$s/%7Bz%7D/%7Bx%7D/%7By%7D/256/png8?app_id=%2$s&app_code=%3$s&ppi=320&lg=%4$s`
  - `http://ad.madvertise.de/sync.html?scheme=`
  - `http://loopme.me/api/v2/events?et=INFO`
  - `http://loopme.me/api/v2/events?et=INFO&vt=`
  - `http://panel.veeso.co:5200/validate?key=identifiers.`

  - http://play.google.com/store/apps/details?id=com.facebook.orca
  - http://search.spotxchange.com/vast/2.00/85394?VPI=MP4
  - http://twitter.com/home?status=
  - http://wv-staging-proxy.appspot.com/proxy?provider=YouTube&video_id=
  - https://m.google.com/app/plus/x/?v=compose&content=
  - https://play.google.com/store/apps/details?id=
  - https://www.facebook.com/dialog/feed?app_id=181821551957328&link=
  - https://www.tumblr.com/oauth/authorize?oauth_token=%s
  - https://www.youtube.com/watch?v=
  - market://details?id=
  - market://details?id=com.facebook.orca

- Communication endpoints is a list of all potential communication endpoints Appicaptor was able to detect. This allows quick enumeration of suspicious domains, raw IP Addresses, etc..
- Communication endpoints: .facebook.com, 1.aerial.maps.api.here.com, 71iapp-cp.nuggad.net, a.applovin.com, ad.71i.de, ad.madvertise.de, adlog.flurry.com, admarvel.s3.amazonaws.com, ads.flurry.com, ak-ns.sascdn.com, amazon-adsystem.amazon.com, amazon-adsystem.com, analytics.query.yahoo.com, android.rwds2.wetter.com, api.netatmo.net, api.tumblr.com, baseurl.admarvel.com, cdn.flurry.com, code.jquery.com, csi.gstatic.com, cv.apprupt.com, d.applovin.com, data.flurry.com, facebook.com, gadgets.wetter.com, googleads.g.doubleclick.net, graph-video.%s, graph.%s, jdom.org, loghost.aatkit.com, loopme.me, ls1.wettercomassets.com, m.google.com, maps.google, mobile.smartadserver.com, nugg.ad, pagead2.googlesyndication.com, panel.veeso.co, play.google.com, playready.directtaps.net, proton.flurry.com, rt.applovin.com, sayt.wettercomassets.com, sb-ssl.google.com, sdk-rh.admarvel.com, sdk.hockeyapp.net, search.spotxchange.com, secure-

rwds2.wetter.com, t1.wettercomassets.com, twitter.com, veeplay.com, vid.applovin.com, wv-staging-proxy.appspot.com, www.agof.de, www.amazon.com, www.facebook.com, www.googleapis.com, www.iab.net, www.madvertise.com, www.netatmo.com, www.tumblr.com, www.wetter.com, www.youtube.com

- App communicates with servers in 8 countries.
- Communication with country: Austria, Netherlands, United States, Ireland, United Kingdom, France, Germany, unknown
- Usage of SSL/TLS can protect the App's communication from adversaries. Tests indicate that communication is at least partly protected with SSL/TLS.
- Mixed usage of HTTP and HTTPS: Protected and unprotected submission of parameters to the same domain. Indicates implementation flaw or weak communication protection.
- App uses the secure default SSL/TLS implementation for client communication. Error-prone modifications were not detected.
- Modifications of the SSL error handling detected: Class WebViewClient is extended and onReceivedSslError(...) is overwritten.
- The app loads the following HTML files via unprotected communication (http), which can be exploited by attackers to remotely change the displayed content and functionality of the app:
  - http://twitter.com/home?status=
  - http://rt.applovin.com/pix
  - http://ad.madvertise.de/action/
  - http://ad.madvertise.de/site/
  - http://ls1.wettercomassets.com/thumbnails/entryId/
  - http://gadgets.wetter.com/android/meta/privacy_en.html
  - http://www.agof.de/datenschutz-mobile/
  - http://wv-staging-proxy.appspot.com/proxy?provider=YouTube&video_id=
  - http://www.agof.de/datenschutz/mobile
  - http://ad.madvertise.de/sync.html
  - http://panel.veeso.co:5200/track

  - http://1.aerial.maps.api.here.com//maptile/2.1/maptile/newest/%1$s/%7Bz%7D/%7Bx%7D/%7By%7D/256/png8?app_id=%2$s&app_code=%3$s&ppi=320&lg=%4$s
  - http://sdk-rh.admarvel.com/adhistory/upload?
  - http://gadgets.wetter.com/android/meta/privacy_de.html
  - http://admarvel.s3.amazonaws.com/sdk/assets/adm_bmp/
  - http://loopme.me/api/v2/events?et=INFO
  - http://gadgets.wetter.com/android/hilfe/
  - http://www.amazon.com/gp/mas/get-appstore/android/ref=mas_mx_mba_iap_dl
  - http://loopme.me/api/v2/events?et=INFO&vt=
  - http://ls1.wettercomassets.com/mobile/android/icons/menu/%1$s/%2$s/%3$s
  - http://www.tumblr.com/connect/login_success.html
  - http://jdom.org/jaxp/xpath/jdom
  - http://search.spotxchange.com/vast/2.00/85394?VPI=MP4
  - http://ad.madvertise.de/sync.html?scheme=
  - http://www.wetter.com/wettercom-live/
  - http://nugg.ad/de/datenschutz/inapp-consumers.html
  - http://gadgets.wetter.com/android/help/
  - http://www.wetter.com/wettertv/

- The app loads the following JavaScript files via unprotected communication (http), which can be exploited by attackers to remotely change the displayed content and functionality of the app:
  - http://admarvel.s3.amazonaws.com/js/admarvel_mraid_v2_complete.js
  - http://ak-ns.sascdn.com/diff/templates/js/mobile/mraid/bridges/android-sdk-mraid-bridge-2.3.js

  - http://code.jquery.com/jquery-latest.min.js
  - http://admarvel.s3.amazonaws.com/js/admarvel_compete_v1.1.js
  - http://baseurl.admarvel.com/mraid.js

- The unprotected communication of the App via http connections can be eavesdroped or maliciously modified.
  - http://1.aerial.maps.api.here.com//maptile/2.1/maptile/newest/%1$s/%7Bz%7D/%7Bx%7D/%7By%7D/256/png8?app_id=%2$s&app_code=%3$s&ppi=320&lg=%4$s
  - http://ad.madvertise.de/sync.html?scheme=
  - http://loopme.me/api/v2/events?et=INFO
  - http://loopme.me/api/v2/events?et=INFO&vt=
  - http://panel.veeso.co:5200/validate?key=identifiers.
  - http://play.google.com/store/apps/details?id=com.facebook.orca
  - http://search.spotxchange.com/vast/2.00/85394?VPI=MP4
  - http://twitter.com/home?status=
  - http://wv-staging-proxy.appspot.com/proxy?provider=YouTube&video_id=

Data security

- ECB mode usage identified. This mode has the disadvantage, that identical plaintext blocks are encrypted into identical ciphertext blocks. Therefore it does not hide patterns well and this mode is not recommended for use in cryptographic protocols at all. Usage of RSA was identified. RSA without padding is considered weak.
- It is considered as a bad practice to use hard-coded cryptographic keys in the application. The following hard-coded cryptographic keys were found:
  - -6,98,68,-94,-105,-92,-70,3,46,-119,-34,-101,119,-13,-94,-7
- The application requires the following permissions from the protection-level: NORMAL

  - ACCESS-WIFI-STATE (Allows applications to access information about Wi-Fi networks)
  - RECEIVE-BOOT-COMPLETED (Allows an application to receive the android.content.Intent ACTION-BOOT-COMPLETED that is broadcast after the system finishes booting. If you don't request this permission, you will not receive the broadcast at that time. Though holding this permission does not have any security implications, it can have a negative impact on the user experience by increasing the amount of time it takes the system to start and allowing applications to have themselves running without the user being aware of them. As such, you must explicitly declare your use of this facility to make that visible to the user.)
  - ACCESS-NETWORK-STATE (Allows applications to access information about networks.)
  - VIBRATE (Allows access to the vibrator.)
  - WAKE-LOCK (Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming.)

- The application requires the following permissions from the protection-level: DANGEROUS
  - ACCESS-COARSE-LOCATION (Allows an app to access approximate location derived from network location sources such as cell towers and Wi-Fi.)
  - ACCESS-FINE-LOCATION (Allows an app to access precise location from location sources such as GPS, cell towers, and Wi-Fi.)
  - INTERNET (Allows applications to open network sockets.)
- Application uses userdefined permissions. Application can access data of a foreign application which requires this permission to access data.
- No indicators for overprivilege/redundant permissions found! The defined permission can not abused by foreign apps.
- The application uses a content provider for interacting with data set structures. Content providers are the standard interface that connects data in one process with code running in another process.
- Every ContentProvider defined in the application is protected by a permission. To access the interface from an external application it must request access to it. The interface is only available if an application defines these permissions.
- Indicator for JavaScript bridge to Android API usage found. JavaScript used in the application (localy stored or loaded dynamicaly) may access and execute Android SDK API calls.

- Wifi-Direct is not enabled. There is no risk for exploiting a vulnerability in the wpa-supplicant module responsible for the wlan management. (http://www.coresecurity.com/advisories/android-wifi-direct-denial-service)

Input interface security

- No indicators for file handling found. The app does not define a filter scheme to process specific files.
- The app does not use protection measures for preventing screenshots. For apps displaying sensitive data it is recommended to disable screenshots.
- The application is vulnerable to tapjacking. When the protection is not used inside an exported activity another application is able to redirect touch events to the exported activity without the users consent.

Privacy

- The Application gathers a list of installed applications. Even though some legitimate applications may use this functionality, it can be misused to send this information to third parties.
- Code obfuscation techniques were detected for the app.
- Obfuscation levels are rated as LOW, MEDIUM, ABOVE MEDIUM, HIGH or UNKNOWN. The detected obfuscation level of HIGH provides sophisticated protection against manual analysis which requires a high effort and deep knowledge to reverse the functionality of the app.
- Device administration features not used.
- Application reads out different unique device Ids. These unique identifiers allows to identify the device and to distinguish it from other devices. Another option for reading out these IDs allow to determine the environment. The application can determine if it is running on a real device or on a virtual/emulated device.
- Accessed unique identifier(s): `build model`, `build manufacturer`, `build product`, `build serial`, `build display`, `build brand`, `IMEI/MEID`, `SIM card serial`, `Wifi-MAC address`, `unique Android ID`
- Indicators for usage of advertisement/tracking framework were found.
- Advertisment-/tracking frameworks found: `AdMarvel`, `Amazon Ad System`, `AppLovin`, `Doubleclick`, `Flurry`, `HockeyApp`, `Madvertise`, `SmartAdServer`

- The application contains no specific exported activity. The application has only launchable activities which are implicit exported. This means there are no activities which can be accessed by an external application. The start activity is:
  - `com.wetter.androidclient.BaseActivity`
- In this application the allow backup option is enabled. This means the application and all application data will be included when performing a device backup. In case the application contains sensitive information these can be extracted from the backup archive or cloned onto other devices.
- Logging statements found in app. This might leak security or privacy relevant information.
- Permission READ-CONTACTS not used.
- Application reads information from different Sensors. This allows the application to track the user and/or determine the environment of the user. There was no Permission defined for camera usage, but the application contains specific API calls accessing the camera.Missing permissions despite of API calls could be an indication for missconfiguration or plugin/library code which is not used. For more detailed information application has to be reviewed manually.
- World readable/writable preference files detected which can be read/written by other applications.
  - WORLD-READABLE

Runtime Security

- The application does not contain a scheduled alarm.
- Indicators found for dynamic code loading. The application loads executable code during runtime from a local or external source.
- Android dalvik code is loaded dynamically by the listed methods.
- In the AndroidManifest.xml file the debuggable option is disabled. This prevents some attempts for debugging the application over the adb debug bridge with jdb. Depending of the used Android operating system this flag is not mandatory, in custom ROMs or rooted devices the OS may ignore this flag. On a non stock Android ROM this can still be misused for dynamic analyzes of the application or for doing runtime manipulation. This option should be disabled in released applications.
- The app is signed with a key that has a strength of 1024 bits. Google recommends to use a key with a strength of 2048 bit or more.
- Loadable libraries found:

  - ARMv8 64 bit: lib/arm64-v8a/libMaply.so
  - ARMv8 64 bit: lib/arm64-v8a/libgnustl_shared.so
  - ARM 32 bit: lib/armeabi-v7a/libMaply.so
  - ARM 32 bit: lib/armeabi-v7a/libgnustl_shared.so
  - ARM 32 bit: lib/armeabi/libMaply.so
  - ARM 32 bit: lib/armeabi/libgnustl_shared.so
  - MIPS I: lib/mips/libMaply.so
  - MIPS I: lib/mips/libgnustl_shared.so
  - MIPS I: lib/mips64/libMaply.so
  - MIPS I: lib/mips64/libgnustl_shared.so
  - x86 32bit: lib/x86/libMaply.so
  - x86 32bit: lib/x86/libgnustl_shared.so
  - x86 64bit: lib/x86_64/libMaply.so
  - x86 64bit: lib/x86_64/libgnustl_shared.so

- The Application has the permission to start automatically after booting the device. The application can execute code without userinteraction or prevention.

Test Performance

- Execution time of all tests: 0:01:13.700

3.17 Wetter.de - Regenradar & mehr (Android)

3.17.1 Tests

The following Table 3.18 summarizes the results of the Android app `Wetter.de - Regenradar & mehr` with version *3.6.2*.

Table 3.18: Overview of summarized test results for »Wetter.de - Regenradar & mehr«

App risks for enterprise usage
☐ *Implementation flaws? No.*
☒ *Privacy risks? Yes.*
☒ *Security risks? Yes.*
Blacklisted by policy

☒ *Violations of default policy? Yes.*

Communication security

☒ *Client communication used? Yes.*
☑ *Communication endpoints: 25 entries, see details.*
☑ *Communication with country:* `Netherlands`, `Sweden`, `United States`, `Ireland`, `Germany`
☒ *SSL/TLS used? Yes.*
☐ *Custom SSL/TLS trust manager implemented? No.*
☒ *SSL/TLS using custom error handling? Yes.*
☐ *SSL/TLS using faulty custom error handling? No.*
☒ *SSL/TLS using manual domain name verification? Yes.*
☒ *Unprotected HTML? Yes.*
☒ *Unprotected communication? Yes.*

Data security

☑ *Cryptographic Primitives:* `"AES/CBC/PKCS5Padding"`
☒ *Application needs normal permissions? Yes.*
☒ *Application needs dangerous permissions? Yes.*
☑ *Userdefined permission usage:* `android.permission.DOWNLOAD_WITHOUT_NOTIFICATION`, `de.rtl.wetter.permission.C2D_MESSAGE`, `com.google.android.c2dm.permission.RECEIVE`, `de.rtli.push.permission.C2D_MESSAGE`
☑ *Overprivileged permissions:* `CAMERA`, `READ_EXTERNAL_STORAGE`
☒ *Is application overprivileged? Yes.*
☒ *Application defines content provider? Yes.*
– *Content provider accessible without permission: None.*
☒ *JavaScript to SDK API bridge usage? Yes.*
☐ *WiFi-Direct enabled? No.*

Input interface security

☑ *App can handle documents of mimeType:* `text/html`, `text/plain`
☐ *Screenshot protection used? No.*
☐ *Tap Jacking Protection used? No.*

Privacy

☒ *Obfuscation used? Yes.*
☑ *Obfuscation level is:* `UNKNOWN`
– *Device administration policy entries: None.*
☑ *Accessed unique identifier(s): 13 entries, see details.*
☑ *Advertisment-/tracking frameworks found:* `Bugsnap`, `Doubleclick`, `INFOnline`
☒ *App provides public accessible activities? Yes.*
☒ *Backup of app is allowed? Yes.*

☒	*Log Statement Enabled? Yes.*
☐	*Permission to access address book? No.*
☑	*Sensor usage:* `Camera`, `WIFI-Based Location`, `GPS Location`
☒	*Unprotected map queries? Yes.*
☒	*Unprotected preference files found? Yes.*

Runtime Security

☐	*Scheduled Alarm Manager registered? No.*
☒	*Dynamically loaded code at runtime? Yes.*
☑	*Dynamically loaded code at runtime type(s):* `dalvik.system.DexClassLoader(...)`, `ClassLoader.loadClass(...)`, `load(...)`, `loadLibrary(...)`
☐	*Allow app debugging Flag? No.*
☒	*App uses outdated signature key? Yes.*
☒	*Contains native libraries: Yes.*
☑	*Executed component after Phone Reboot:* `com.microsoft.azure.engagement.reach.EngagementReachReceiver`

3.17.2 Details

The following sections describe details about the test results of `Wetter.de - Regenradar & mehr` with version *3.6.2*.

App risks for enterprise usage

- Reasons for category privacy risks:
  - Unprotected Access: Disclosure of location or web query data though unprotected communication with service providers.
  - Sensor Access: Usage of camera violates rules for detected app type and poses a potential risk by taking photos unnoticed or gaining access to those already stored.
- Reasons for category security risks:
  - Office Data: App can handle office files, which violates security rules for detected app type and poses a potential risk by exposing corporate data to untrusted software.
  - Unprotected Web Content: App loads active web content (e.g. JavaScript or HTML files) without integrity protection. This poses a risk as man-in-the-middle attackers can modify the loaded web content and change the functionality of the app.

Blacklisted by policy

- Reasons for category violations of default policy:
  - Overall consolidated test results indicate a medium risk for enterprise usage originated from this app.
  - Enterprise documents maybe at risk during communication processes with external entities.

Communication security

- Client communication detected. The application can establish a network connection to one or more specific host systems. URLs with parameters found:
  - `http://maps.googleapis.com/maps/api/geocode/json?latlng=%1$f,%2$f&sensor=true&language=%3$s`
  - `https://play.google.com/store/apps/details?id=`
  - `market://details?id=`
  - `market://details?id=com.google.android.gms.ads`
- Communication endpoints is a list of all potential communication endpoints Appicaptor was able to detect. This allows quick enumeration of suspicious domains, raw IP Addresses, etc..
- Communication endpoints: `app-measurement.com`, `app.adjust.com`, `app.wetter.de`, `bugsnag.com`, `config.ioam.de`, `csi.gstatic.com`, `de-ipd.videoplaza.tv`, `de.ioam.de`, `goo.gl`, `googleads.g.doubleclick.net`, `iam-agof-app.irquest.com`, `jabber.org`, `maps.googleapis.com`, `notify.bugsnag.com`, `pagead2.googlesyndication.com`, `partner.rtl.de`, `play.google.com`, `plus.google.com`, `px1.vtrtl.de`, `ssl.google-analytics.com`, `www.google-analytics.com`, `www.google.com`, `www.googleapis.com`, `www.googletagmanager.com`, `www.wetter.de`
- App communicates with servers in 5 countries.
- Usage of SSL/TLS can protect the App's communication from adversaries. Tests indicate that communication is at least partly protected with SSL/TLS.
- App uses the secure default SSL/TLS implementation for client communication. Error-prone modifications were not detected.

- Modifications of the SSL error handling detected: Class WebViewClient is extended and onReceivedSslError(...) is overwritten.
- Correct verification of the corresponding client hostname is important for SSL/TLS security. The app changes the secure default hostname verification by the following:
  - Interface HostnameVerifier is implemented or extended.
- The app loads the following HTML files via unprotected communication (http), which can be exploited by attackers to remotely change the displayed content and functionality of the app:
  - `http://jabber.org/protocol/geoloc`
  - `http://maps.googleapis.com/maps/api/geocode/json?latlng=%1$f,%2$f&sensor=true&language=%3$s`
- The unprotected communication of the App via http connections can be eavesdroped or maliciously modified.
  - `http://maps.googleapis.com/maps/api/geocode/json?latlng=%1$f,%2$f&sensor=true&language=%3$s`

Data security

- The application requires the following permissions from the protection-level: NORMAL
  - READ-EXTERNAL-STORAGE (Allows an application to read from external storage. Any app that declares the WRITE-EXTERNAL-STORAGE permission is implicitly granted this permission. Currently, this permission is not enforced and all apps still have access to read from external storage without this permission. That will change in a future release and apps will require this permission to read from external storage. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
  - VIBRATE (Allows access to the vibrator.)
  - ACCESS-NETWORK-STATE (Allows applications to access information about networks.)

  - RECEIVE-BOOT-COMPLETED (Allows an application to receive the android.content.Intent ACTION-BOOT-COMPLETED that is broadcast after the system finishes booting. If you don't request this permission, you will not receive the broadcast at that time. Though holding this permission does not have any security implications, it can have a negative impact on the user experience by increasing the amount of time it takes the system to start and allowing applications to have themselves running without the user being aware of them. As such, you must explicitly declare your use of this facility to make that visible to the user.)
  - WAKE-LOCK (Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming.)
  - ACCESS-WIFI-STATE (Allows applications to access information about Wi-Fi networks)

- The application requires the following permissions from the protection-level: DANGEROUS
  - ACCESS-FINE-LOCATION (Allows an app to access precise location from location sources such as GPS, cell towers, and Wi-Fi.)
  - CAMERA (Required to be able to access the camera device. This will automatically enforce the uses-feature manifest element for all camera features. If you do not require all camera features or can properly operate if a camera is not available, then you must modify your manifest as appropriate in order to install on devices that don't support all camera features.)
  - BLUETOOTH (Allows applications to connect to paired Bluetooth devices.)
  - WRITE-EXTERNAL-STORAGE (Allows an application to write to external storage. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
  - INTERNET (Allows applications to open network sockets.)
  - ACCESS-COARSE-LOCATION (Allows an app to access approximate location derived from network location sources such as cell towers and Wi-Fi.)

- Application uses userdefined permissions. Application can access data of a foreign application which requires this permission to access data.
- Application is propably overprivileged. Application has too much permissions. Foreign applications may be able to abuse this permission.

- The application uses a content provider for interacting with data set structures. Content providers are the standard interface that connects data in one process with code running in another process.
- Every ContentProvider defined in the application is protected by a permission. To access the interface from an external application it must request access to it. The interface is only available if an application defines these permissions.
- Indicator for JavaScript bridge to Android API usage found. JavaScript used in the application (localy stored or loaded dynamicaly) may access and execute Android SDK API calls.
- Wifi-Direct is not enabled. There is no risk for exploiting a vulnerability in the wpa-supplicant module responsible for the wlan management. (http://www.coresecurity.com/advisories/android-wifi-direct-denial-service)

Input interface security

- The application or application components define specific type filter for handling different file types. If different applications define the same filter types the user has to decide which application should handle the file.
- The app does not use protection measures for preventing screenshots. For apps displaying sensitive data it is recommended to disable screenshots.
- The application is vulnerable to tapjacking. When the protection is not used inside an exported activity another application is able to redirect touch events to the exported activity without the users consent.

Privacy

- Code obfuscation techniques were detected for the app.
- The obfuscation level UNKNOWN means that the application has the capability to dynamically load code from outside, which currently is not part of the analysis. Therefore, the obfuscation strength is not evaluated.
- Device administration features not used.
- Application reads out different unique device Ids. These unique identifiers allows to identify the device and to distinguish it from other devices. Another option for reading out these IDs allow to determine the environment. The application can determine if it is running on a real device or on a virtual/emulated device.

- Accessed unique identifier(s): `build model`, `build manufacturer`, `build product`, `build serial`, `build hardware`, `build display`, `build fingerprint`, `build brand`, `IMEI/MEID`, `Wifi-MAC address`, `country code + mobile network code for SIM provider`, `MMC (Mobile Country Code)`, `unique Android ID`
- Indicators for usage of advertisement/tracking framework were found.
- The application contains components (Activities) which are exported. This means these parts of the application are accessible or executable by other applications. An external app can write or read information/data to or from this app. Additionally components of this application can be executed. Following Activities are exported:
  - `com.microsoft.azure.engagement.reach.activity.EngagementWebAnnouncementActivity`
  - `com.microsoft.azure.engagement.reach.activity.EngagementTextAnnouncementActivity`
  - `com.microsoft.azure.engagement.reach.activity.EngagementPollActivity`
  - `com.microsoft.azure.engagement.reach.activity.EngagementLoadingActivity`
  - `de.rtl.wetter.views.activities.HomeActivity`
  - `de.rtl.wetter.views.activities.DeeplinkActivity`
- In this application the allow backup option is enabled. This means the application and all application data will be included when performing a device backup. In case the application contains sensitive information these can be extracted from the backup archive or cloned onto other devices.
- Logging statements found in app. This might leak security or privacy relevant information.
- Permission READ-CONTACTS not used.
- Application reads information from different sensors. This allows the application to track the user and/or determine the environment of the user.
- App contains URL(s) that indicate an unprotected HTTP access to map providers. The transmitted location query parameters to the following map providers are in this case accesible by third parties:
  - Google Maps

- World readable/writable preference files detected which can be read/written by other applications.
  - WORLD-READABLE

Runtime Security

- The application does not contain a scheduled alarm.
- Indicators found for dynamic code loading. The application loads executable code during runtime from a local or external source.
- Android dalvik code is loaded dynamically by the listed methods. Native code by Java Native Interface (for dynamic loading) is used.
- In the AndroidManifest.xml file the debuggable option is disabled. This prevents some attempts for debugging the application over the adb debug bridge with jdb. Depending of the used Android operating system this flag is not mandatory, in custom ROMs or rooted devices the OS may ignore this flag. On a non stock Android ROM this can still be misused for dynamic analyzes of the application or for doing runtime manipulation. This option should be disabled in released applications.
- The app is signed with a key that has a strength of 1024 bits. Google recommends to use a key with a strength of 2048 bit or more.
- Loadable libraries found:
  - `ARM 32 bit: lib/armeabi/librealm-jni.so`
  - `x86 32bit: lib/x86/librealm-jni.so`
  - `ARMv8 64 bit: lib/arm64-v8a/librealm-jni.so`
  - `ARM 32 bit: lib/armeabi-v7a/librealm-jni.so`
  - `x86 64bit: lib/x86_64/librealm-jni.so`
  - `MIPS I: lib/mips/librealm-jni.so`
- The Application has the permission to start automatically after booting the device. The application can execute code without userinteraction or prevention.

Test Performance

- Execution time of all tests: 0:01:29.156

3.18 wetter.info (Android)

3.18.1 Tests

The following Table 3.19 summarizes the results of the Android app `wetter.info` with version *1.7.7*.

Table 3.19: Overview of summarized test results for »wetter.info«

App risks for enterprise usage	
☐	*Implementation flaws? No.*
☐	*Privacy risks? No.*
☒	*Security risks? Yes.*
Blacklisted by policy	
☐	*Violations of default policy? No.*
Communication security	
☒	*Client communication used? Yes.*
☑	*Communication endpoints: 36 entries, see details.*
☑	*Communication with country:* `United States`, `Ireland`, `Germany`
☒	*SSL/TLS used? Yes.*
☐	*Custom SSL/TLS trust manager implemented? No.*
☒	*SSL/TLS using custom error handling? Yes.*
☐	*SSL/TLS using faulty custom error handling? No.*
☐	*SSL/TLS using manual domain name verification? No.*
☒	*Unprotected HTML? Yes.*
Data security	
☒	*Application needs normal permissions? Yes.*
☒	*Application needs dangerous permissions? Yes.*
☑	*Overprivileged permissions:* `READ-EXTERNAL-STORAGE`
☒	*Is application overprivileged? Yes.*
☒	*JavaScript to SDK API bridge usage? Yes.*
☐	*WiFi-Direct enabled? No.*
Input interface security	
⊟	*App can handle documents of mimeType: None.*
☐	*Screenshot protection used? No.*
☐	*Tap Jacking Protection used? No.*
Privacy	
☒	*Obfuscation used? Yes.*
☑	*Obfuscation level is:* `UNKNOWN`
⊟	*Device administration policy entries: None.*
☑	*Accessed unique identifier(s): 9 entries, see details.*

☑	*Advertisment-/tracking frameworks found:* `Adjust`, `HockeyApp`, `INFOnline`
☒	*App provides public accessible activities? Yes.*
☒	*Backup of app is allowed? Yes.*
☒	*Log Statement Enabled? Yes.*
☐	*Permission to access address book? No.*
☑	*Sensor usage:* `GPS Location`, `Acceleration/Light`

Runtime Security	
☒	*Scheduled Alarm Manager registered? Yes.*
☑	*Alarm repeating types:* `RTC`
☒	*Alarm intervals dynamically? Yes.*
☐	*Alarm Manager initialized dynamically? No.*
☒	*Dynamically loaded code at runtime? Yes.*
☑	*Dynamically loaded code at runtime type(s):* `ClassLoader.loadClass(...)`
☐	*Allow app debugging Flag? No.*
☐	*Allow autoexecute after Phone Reboot? No.*
☒	*App uses outdated signature key? Yes.*

3.18.2 Details

The following sections describe details about the test results of `wetter.info` with version *1.7.7*.

App risks for enterprise usage

- Reasons for category security risks:
  - Unprotected Web Content: App loads active web content (e.g. JavaScript or HTML files) without integrity protection. This poses a risk as man-in-the-middle attackers can modify the loaded web content and change the functionality of the app.

Communication security

- Client communication detected. The application can establish a network connection to one or more specific host systems. URLs with parameters found:
  - `WEATHER_REPORT_CONTENT_BASE_URL=http://tomo.potter.t-online.de/mcp_dev/index.php?r=businesslogic/wetter/w_v1_0_0/news/getContentAsJson&url=`

  - WEATHER_REPORT_CONTENT_BASE_URL=https://mcp.t-online.de/index.php?r=businesslogic/wetter/w_v1_0_0/news/getContentAsJson&url=
  - WEATHER_REPORT_PORTAL_URL=http://tomo.potter.t-online.de/mcp_dev/index.php?r=businesslogic/wetter/w_v1_0_0/news/getPortalAsJson
  - WEATHER_REPORT_PORTAL_URL=https://mcp.t-online.de/index.php?r=businesslogic/wetter/w_v1_0_0/news/getPortalAsJson
  - https://play.google.com/store/apps/details?id=de.telekom.t_online_de&hl=de
  - %7B0%7D://%7B1%7D%7B2%7D/adevent?mpid=%7B3%7D&deliveryID=%7B4%7D&event=%7B5%7D&mediationPartnerId=%7B6%7D
  - %7B0%7D://%7B1%7D%7B2%7D/adevent?network=%7B3%7D.%7B4%7D&alias=%7B5%7D&deliveryID=%7B6%7D&event=%7B7%7D&mediationPartnerId=%7B8%7D

- Communication endpoints is a list of all potential communication endpoints Appicaptor was able to detect. This allows quick enumeration of suspicious domains, raw IP Addresses, etc..
- Communication endpoints: accounts.google.com, app.adjust.io, config.ioam.de, de.ioam.de, iam-agof-app.irquest.com, login.live.com, login.yahoo.com, play.google.com, plus.google.com, sdk.hockeyapp.net, twitter.com, www.alertas-tiempo.es, www.centrometeo.pt, www.facebook.com, www.google.de, www.googleapis.com, www.interactivemedia.net, www.linkedin.com, www.meteo-allerta.it, www.meteo-info.be, www.meteocentrale.ch, www.meteocentrale.li, www.meteozentral.lu, www.noodweercentrale.nl, www.paypal.com, www.saa-varoitukset.fi, www.severe-weather-centre.co.uk, www.severe-weather-ireland.com, www.t-online.de, www.unwetterzentrale.de, www.vader-alarm.se, www.vaer-sentral.no, www.vejrcentral.dk, www.vigilance-meteo.fr, www.wetteralarm.at, www.wikipedia.org
- App communicates with servers in 3 countries.

- Usage of SSL/TLS can protect the App's communication from adversaries. Tests indicate that communication is at least partly protected with SSL/TLS.
- App uses the secure default SSL/TLS implementation for client communication. Error-prone modifications were not detected.
- Modifications of the SSL error handling detected: Class WebViewClient is extended and onReceivedSslError(...) is overwritten.
- The app loads the following HTML files via unprotected communication (http), which can be exploited by attackers to remotely change the displayed content and functionality of the app:
  - `http://iam-agof-app.irquest.com/agof-qds/v2`
  - `http://iam-agof-app.irquest.com/agof-qds/v2/measure`

Data security

- The application requires the following permissions from the protection-level: NORMAL
  - ACCESS-WIFI-STATE (Allows applications to access information about Wi-Fi networks)
  - READ-EXTERNAL-STORAGE (Allows an application to read from external storage. Any app that declares the WRITE-EXTERNAL-STORAGE permission is implicitly granted this permission. Currently, this permission is not enforced and all apps still have access to read from external storage without this permission. That will change in a future release and apps will require this permission to read from external storage. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
  - ACCESS-NETWORK-STATE (Allows applications to access information about networks.)
- The application requires the following permissions from the protection-level: DANGEROUS
  - INTERNET (Allows applications to open network sockets.)
  - ACCESS-FINE-LOCATION (Allows an app to access precise location from location sources such as GPS, cell towers, and Wi-Fi.)
  - WRITE-EXTERNAL-STORAGE (Allows an application to write to external storage. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)

- Application is propably overprivileged. Application has too much permissions. Foreign applications may be able to abuse this permission.
- Indicator for JavaScript bridge to Android API usage found. JavaScript used in the application (localy stored or loaded dynamicaly) may access and execute Android SDK API calls.
- Wifi-Direct is not enabled. There is no risk for exploiting a vulnerability in the wpa-supplicant module responsible for the wlan management. (http://www.coresecurity.com/advisories/android-wifi-direct-denial-service)

Input interface security

- No indicators for file handling found. The app does not define a filter scheme to process specific files.
- The app does not use protection measures for preventing screenshots. For apps displaying sensitive data it is recommended to disable screenshots.
- The application is vulnerable to tapjacking. When the protection is not used inside an exported activity another application is able to redirect touch events to the exported activity without the users consent.

Privacy

- Code obfuscation techniques were detected for the app.
- The obfuscation level UNKNOWN means that the application has the capability to dynamically load code from outside, which currently is not part of the analysis. Therefore, the obfuscation strength is not evaluated.
- Device administration features not used.
- Application reads out different unique device Ids. These unique identifiers allows to identify the device and to distinguish it from other devices. Another option for reading out these IDs allow to determine the environment. The application can determine if it is running on a real device or on a virtual/emulated device.
- Accessed unique identifier(s): `build model`, `build manufacturer`, `build product`, `build hardware`, `build brand`, `IMEI/MEID`, `Wifi-MAC address`, `country code + mobile network code for SIM provider`, `unique Android ID`
- Indicators for usage of advertisement/tracking framework were found.

- The application contains components (Activities) which are exported. This means these parts of the application are accessible or executable by other applications. An external app can write or read information/data to or from this app. Additionally components of this application can be executed. Following Activities are exported:
  - `com.telekom.wetterinfo.ui.activities.WidgetConfigurationActivity`
- In this application the allow backup option is enabled. This means the application and all application data will be included when performing a device backup. In case the application contains sensitive information these can be extracted from the backup archive or cloned onto other devices.
- Logging statements found in app. This might leak security or privacy relevant information.
- Permission READ-CONTACTS not used.
- Application reads information from different sensors. This allows the application to track the user and/or determine the environment of the user.

Runtime Security

- The application contains a registered scheduled alarm. With such an alarm the application repeats the execution of the registered task for example every 10 hours. The following classes register scheduled tasks:
  - `com.telekom.wetterinfo.ui.widgets.LocationWidgetBase`
- The scheduled task gets repeated in the following intervals:
  - Dynamic interval(s)
- The alarm manager has been initialized properly.
- Indicators found for dynamic code loading. The application loads executable code during runtime from a local or external source.
- Android dalvik code is loaded dynamically by the listed methods.
- In the AndroidManifest.xml file the debuggable option is disabled. This prevents some attempts for debugging the application over the adb debug bridge with jdb. Depending of the used Android operating system this flag is not mandatory, in custom ROMs or rooted devices the OS may ignore this flag. On a non stock Android ROM this can still be misused for dynamic analyzes of the application or for doing runtime manipulation. This option should be disabled in released applications.

- The app is signed with a key that has a strength of 1024 bits. Google recommends to use a key with a strength of 2048 bit or more.

Test Performance

- Execution time of all tests: 0:00:27.412

3.19 WetterOnline (Android)

3.19.1 Tests

The following Table 3.20 summarizes the results of the Android app `WetterOnline` with version *3.14.3*.

Table 3.20: Overview of summarized test results for »WetterOnline«

App risks for enterprise usage	
☒	*Implementation flaws? Yes.*
☒	*Privacy risks? Yes.*
☒	*Security risks? Yes.*
Blacklisted by policy	
☒	*Violations of default policy? Yes.*
Communication security	
☒	*Client communication used? Yes.*
☑	*Communication endpoints: 40 entries, see details.*
☑	*Communication with country:* `Netherlands`, `United States`, `Ireland`, `Germany`, `unknown`
☒	*SSL/TLS used? Yes.*
☑	*Domains accessed with http AND https:* `play.google.com`
☒	*Custom SSL/TLS trust manager implemented? Yes.*
☐	*Faulty custom SSL/TLS trust manager implemented? No.*
☒	*SSL/TLS using custom error handling? Yes.*
☐	*SSL/TLS using faulty custom error handling? No.*
☒	*SSL/TLS using manual domain name verification? Yes.*
☒	*Unprotected HTML? Yes.*
☒	*Unprotected communication? Yes.*
Data security	
☑	*Cryptographic Primitives:* `"AES/CBC/PKCS5Padding"`
☒	*Application needs normal permissions? Yes.*
☒	*Application needs dangerous permissions? Yes.*

☑ *Userdefined permission usage:* `com.android.vending.BILLING`, `de.wetteronline.wetterapp.permission.C2D-MESSAGE`, `com.google.android.c2dm.permission.RECEIVE`, `com.google.android.providers.gsf.permission.READ-GSERVICES`
☑ *Overprivileged permissions:* `READ-EXTERNAL-STORAGE`
☒ *Is application overprivileged? Yes.*
☒ *Application defines content provider? Yes.*
⊟ *Content provider accessible without permission: None.*
☒ *JavaScript to SDK API bridge usage? Yes.*
☐ *WiFi-Direct enabled? No.*

Input interface security

⊟ *App can handle documents of mimeType: None.*
☐ *Screenshot protection used? No.*
☐ *Tap Jacking Protection used? No.*

Privacy

☒ *Installed app list accessed? Yes.*
☒ *Obfuscation used? Yes.*
☑ *Obfuscation level is:* `HIGH`
⊟ *Device administration policy entries: None.*
☑ *Accessed unique identifier(s): 11 entries, see details.*
☑ *Advertisment-/tracking frameworks found:* `Crashlytics`, `Doubleclick`, `INFOnline`
☒ *App provides public accessible activities? Yes.*
☒ *Backup of app is allowed? Yes.*
☒ *Log Statement Enabled? Yes.*
☐ *Permission to access address book? No.*
☒ *Remote auto backup with include enabled? Yes.*
☑ *Sensor usage:* `Camera`, `WIFI-Based Location`, `GPS Location`
☒ *Unprotected preference files found? Yes.*

Runtime Security

☒ *Scheduled Alarm Manager registered? Yes.*
☑ *Alarm repeating types:* `RTC`
☐ *Alarm intervals dynamically? No.*
☐ *Alarm Manager initialized dynamically? No.*
☒ *Dynamically loaded code at runtime? Yes.*
☑ *Dynamically loaded code at runtime type(s):* `dalvik.system.DexClassLoader(...)`, `ClassLoader.loadClass(...)`
☐ *Allow app debugging Flag? No.*
☑ *Executed component after Phone Reboot:* `de.wetteronline.lib.wetterapp.background.BackgroundReceiver`

3.19.2 Details

The following sections describe details about the test results of `WetterOnline` with version *3.14.3*.

App risks for enterprise usage

- Reasons for category implementation flaws:
  - Possible flaw: unintended use of insecure HTTP protocol for transmissions of parameters to servers capable of HTTPS.
- Reasons for category privacy risks:
  - Sensor Access: Usage of camera violates rules for detected app type and poses a potential risk by taking photos unnoticed or gaining access to those already stored.
  - App Listing: Usage of detected functionality to access list of installed apps poses a privacy risk for detected app type.
- Reasons for category security risks:
  - Unprotected Web Content: App loads active web content (e.g. JavaScript or HTML files) without integrity protection. This poses a risk as man-in-the-middle attackers can modify the loaded web content and change the functionality of the app.

Blacklisted by policy

- Reasons for category violations of default policy:
  - Estimated overall app risk for the enterprise exceeds the security policy threshold due to detected risks and flaws exploitable by skilled attackers without the existence of additional supporting factors.

Communication security

- Client communication detected. The application can establish a network connection to one or more specific host systems. URLs with parameters found:
  - `amzn://apps/android?p=`
  - `amzn://apps/android?p=%s`
  - `amzn://apps/android?p=de.wetteronline.regenradar`
  - `amzn://apps/android?p=de.wetteronline.regenradarpro`

- amzn://apps/android?p=de.wetteronline.wetterapp
- amzn://apps/android?p=de.wetteronline.wetterappamzn
- amzn://apps/android?p=de.wetteronline.wetterapppro
- amzn://apps/android?p=de.wetteronline.wettermaps
- http://agof.de/datenschutz-allgemein/?lang=en
- http://m.wetteronline.de/android/?ADF=1
- http://m.wetteronline.de/android/?ADF=4
- http://m.wetteronline.de/cgi-bin/start?ADF=1
- http://m.wetteronline.de/cgi-bin/start?ADF=4
- http://play.google.com/store/apps/details?id=
- http://play.google.com/store/apps/details?id=com.facebook.orca
- http://wetteronline.de/wetterticker?postId=
- http://www.amazon.de/gp/mas/dl/android?p=
- http://www.amazon.de/gp/mas/dl/android?p=%s
- http://www.amazon.de/gp/mas/dl/android?p=de.wetteronline.regenradar
- http://www.amazon.de/gp/mas/dl/android?p=de.wetteronline.regenradarpro
- http://www.amazon.de/gp/mas/dl/android?p=de.wetteronline.wetterapp
- http://www.amazon.de/gp/mas/dl/android?p=de.wetteronline.wetterappamzn
- http://www.amazon.de/gp/mas/dl/android?p=de.wetteronline.wetterapppro
- http://www.amazon.de/gp/mas/dl/android?p=de.wetteronline.wettermaps
- http://www.wetteronline.at/?ireq=true&pid=p_search&searchpcid=external&searchstring=%s

- http://www.wetteronline.ch/?ireq=true&pid=p_search&searchpcid=external&searchstring=%s
- http://www.wetteronline.de/?ireq=true&pid=p_search&searchpcid=external&searchstring=%s
- http://www.wetteronline.de/datenschutz?lang=en
- https://play.google.com/store/apps/details?id=%s&referrer=utm_source3Dwetteronline.app26utm_medium3D%s
- market://details?id=
- market://details?id=%s&referrer=utm_source3Dwetteronline.app26utm_medium3D%s
- market://details?id=com.facebook.orca
- market://details?id=com.google.android.gms.ads
- market://details?id=de.wetteronline.regenradar&referrer=utm_source%3Dwetteronline.app%26utm_medium%3Dwetterapp
- market://details?id=de.wetteronline.regenradarpro&referrer=utm_source%3Dwetteronline.app%26utm_medium%3Dwetterapp
- market://details?id=de.wetteronline.wetterapp&referrer=utm_source%3Dwetteronline.app%26utm_medium%3Dwetterapp
- market://details?id=de.wetteronline.wetterapppro&referrer=utm_source%3Dwetteronline.app%26utm_medium%3Dwetterapp
- market://details?id=de.wetteronline.wettermaps&referrer=utm_source%3Dwetteronline.app%26utm_medium%3Dwetterapp
- market://details?id=de.wetteronline.wetterticker&referrer=utm_source%3Dwetteronline.app%26utm_medium%3Dwetterapp
- ..https://play.google.com/store/apps/details?id=de.wetteronline.regenradar&referrer=utm_source%3Dwetteronline.app%26utm_medium%3Dwettera

  - ..https://play.google.com/store/apps/details?id=de.wetteronline.regenradarpro&referrer=utm_source%3Dwetteronline.app%26utm_medium%3Dwettera
  - ..https://play.google.com/store/apps/details?id=de.wetteronline.wetterapp&referrer=utm_source%3Dwetteronline.app%26utm_medium%3Dwettera
  - ..https://play.google.com/store/apps/details?id=de.wetteronline.wetterapppro&referrer=utm_source%3Dwetteronline.app%26utm_medium%3Dwettera
  - ..https://play.google.com/store/apps/details?id=de.wetteronline.wettermaps&referrer=utm_source%3Dwetteronline.app%26utm_medium%3Dwettera
  - ..https://play.google.com/store/apps/details?id=de.wetteronline.wetterticker&referrer=utm_source%3Dwetteronline.app%26utm_medium%3Dwettera

- Communication endpoints is a list of all potential communication endpoints Appicaptor was able to detect. This allows quick enumeration of suspicious domains, raw IP Addresses, etc..
- Communication endpoints: .facebook.com, agof.de, api-dev.wetteronline.de, api-stage.wetteronline.de, api.wetteronline.de, app-measurement.com, config.ioam.de, csi.gstatic.com, de.ioam.de, disqus.com, e.crashlytics.com, facebook.com, goo.gl, googleads.g.doubleclick.net, graph-video.%s, graph.%s, iam-agof-app.irquest.com, m.wetteronline.de, pagead2.googlesyndication.com, play.google.com, plus.google.com, sb-ssl.google.com, settings.crashlytics.com, ssl.google-analytics.com, st-dev.wetteronline.de, twitter.com, upload.wetteronline.de, wetterapp-1.firebaseio.com, wetteronline.de, www.agma-mmc.de, www.agof.de, www.amazon.de, www.google-analytics.com, www.google.com, www.infonline.de, www.ivw.eu, www.weatherandradar.com, www.wetteronline.at, www.wetteronline.ch, www.wetteronline.de
- App communicates with servers in 5 countries.

- Usage of SSL/TLS can protect the App's communication from adversaries. Tests indicate that communication is at least partly protected with SSL/TLS.
- Mixed usage of HTTP and HTTPS: Protected and unprotected submission of parameters to the same domain. Indicates implementation flaw or weak communication protection.
- Modifications of trust management found. Interface X509TrustManager is implemented or extended.
- Modifications of the SSL error handling detected: Class WebViewClient is extended and onReceivedSslError(...) is overwritten.
- Correct verification of the corresponding client hostname is important for SSL/TLS security. The app changes the secure default hostname verification by the following:
  - Interface HostnameVerifier is implemented or extended.
- The app loads the following HTML files via unprotected communication (http), which can be exploited by attackers to remotely change the displayed content and functionality of the app:
  - `http://www.amazon.de/gp/mas/dl/android?p=`
  - `http://www.wetteronline.de/apps#WetterTicker`
  - `http://www.wetteronline.ch/apps`
  - `http://www.wetteronline.de/uploader`
  - `http://www.wetteronline.ch/datenschutz/`
  - `http://www.wetteronline.ch/apps#WetterApp`
  - `http://www.wetteronline.at/apps`
  - `http://www.wetteronline.de/apps#RegenRadar`
  - `http://wetteronline.de/wetterticker?postId=`
  - `http://m.wetteronline.de/cgi-bin/start?ADF=1`
  - `http://www.wetteronline.at/datenschutz/`
  - `http://www.wetteronline.de/apps#WetterApp`
  - `http://www.wetteronline.ch/apps#WetterRadar`
  - `http://www.wetteronline.de/datenschutz`
  - `http://m.wetteronline.de/cgi-bin/start?ADF=4`
  - `http://www.wetteronline.ch/apps#RegenRadar`
  - `http://www.wetteronline.de/datenschutz/`

  - http://m.wetteronline.de/android/?ADF=4
  - http://m.wetteronline.de/android/?ADF=1
  - http://www.amazon.de/gp/mas/dl/android?p=%s
  - http://www.wetteronline.at/apps#WetterTicker
  - http://www.wetteronline.at/apps#RegenRadar
  - http://www.wetteronline.at/apps#WetterRadar
  - http://www.wetteronline.ch/uploader
  - http://www.wetteronline.de/mitgliedschaft
  - http://www.wetteronline.de/datenschutz?lang=en
  - http://www.wetteronline.at/mitgliedschaft
  - http://agof.de/datenschutz-allgemein/?lang=en
  - http://play.google.com/store/apps/details?id=
  - http://www.agof.de/datenschutz
  - http://www.wetteronline.ch/apps#WetterTicker
  - http://www.wetteronline.de/apps#WetterRadar
  - http://www.wetteronline.at/apps#WetterApp
  - http://www.wetteronline.de/apps
  - http://www.wetteronline.at/uploader
  - http://www.wetteronline.ch/mitgliedschaft

- The unprotected communication of the App via http connections can be eavesdroped or maliciously modified.
  - http://agof.de/datenschutz-allgemein/?lang=en
  - http://m.wetteronline.de/android/?ADF=1
  - http://m.wetteronline.de/android/?ADF=4
  - http://m.wetteronline.de/cgi-bin/start?ADF=1
  - http://m.wetteronline.de/cgi-bin/start?ADF=4
  - http://play.google.com/store/apps/details?id=

  - http://play.google.com/store/apps/details?id=com.facebook.orca
  - http://wetteronline.de/wetterticker?postId=
  - http://www.amazon.de/gp/mas/dl/android?p=
  - http://www.amazon.de/gp/mas/dl/android?p=%s
  - http://www.amazon.de/gp/mas/dl/android?p=de.wetteronline.regenradar
  - http://www.amazon.de/gp/mas/dl/android?p=de.wetteronline.regenradarpro
  - http://www.amazon.de/gp/mas/dl/android?p=de.wetteronline.wetterapp
  - http://www.amazon.de/gp/mas/dl/android?p=de.wetteronline.wetterappamzn
  - http://www.amazon.de/gp/mas/dl/android?p=de.wetteronline.wetterapppro
  - http://www.amazon.de/gp/mas/dl/android?p=de.wetteronline.wettermaps
  - http://www.wetteronline.at/?ireq=true&pid=p_search&searchpcid=external&searchstring=%s
  - http://www.wetteronline.ch/?ireq=true&pid=p_search&searchpcid=external&searchstring=%s
  - http://www.wetteronline.de/?ireq=true&pid=p_search&searchpcid=external&searchstring=%s
  - http://www.wetteronline.de/datenschutz?lang=en

Data security

- The application requires the following permissions from the protection-level: NORMAL
  - READ-EXTERNAL-STORAGE (Allows an application to read from external storage. Any app that declares the WRITE-EXTERNAL-STORAGE permission is implicitly granted this permission. Currently, this permission is not enforced and all apps still have access to read from external storage without this permission. That will change in a future release and apps will require this permission to read from external storage. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)

  - RECEIVE-BOOT-COMPLETED (Allows an application to receive the android.content.Intent ACTION-BOOT-COMPLETED that is broadcast after the system finishes booting. If you don't request this permission, you will not receive the broadcast at that time. Though holding this permission does not have any security implications, it can have a negative impact on the user experience by increasing the amount of time it takes the system to start and allowing applications to have themselves running without the user being aware of them. As such, you must explicitly declare your use of this facility to make that visible to the user.)
  - WAKE-LOCK (Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming.)
  - VIBRATE (Allows access to the vibrator.)
  - ACCESS-NETWORK-STATE (Allows applications to access information about networks.)

- The application requires the following permissions from the protection-level: DANGEROUS
  - ACCESS-FINE-LOCATION (Allows an app to access precise location from location sources such as GPS, cell towers, and Wi-Fi.)
  - WRITE-EXTERNAL-STORAGE (Allows an application to write to external storage. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
  - INTERNET (Allows applications to open network sockets.)
  - ACCESS-COARSE-LOCATION (Allows an app to access approximate location derived from network location sources such as cell towers and Wi-Fi.)
  - CAMERA (Required to be able to access the camera device. This will automatically enforce the uses-feature manifest element for all camera features. If you do not require all camera features or can properly operate if a camera is not available, then you must modify your manifest as appropriate in order to install on devices that don't support all camera features.)
- Application uses userdefined permissions. Application can access data of a foreign application which requires this permission to access data.
- Application is propably overprivileged. Application has too much permissions. Foreign applications may be able to abuse this permission.

- The application uses a content provider for interacting with data set structures. Content providers are the standard interface that connects data in one process with code running in another process.
- Every ContentProvider defined in the application is protected by a permission. To access the interface from an external application it must request access to it. The interface is only available if an application defines these permissions.
- Indicator for JavaScript bridge to Android API usage found. JavaScript used in the application (localy stored or loaded dynamicaly) may access and execute Android SDK API calls.
- Wifi-Direct is not enabled. There is no risk for exploiting a vulnerability in the wpa-supplicant module responsible for the wlan management. (http://www.coresecurity.com/advisories/android-wifi-direct-denial-service)

Input interface security

- No indicators for file handling found. The app does not define a filter scheme to process specific files.
- The app does not use protection measures for preventing screenshots. For apps displaying sensitive data it is recommended to disable screenshots.
- The application is vulnerable to tapjacking. When the protection is not used inside an exported activity another application is able to redirect touch events to the exported activity without the users consent.

Privacy

- The Application gathers a list of installed applications. Even though some legitimate applications may use this functionality, it can be misused to send this information to third parties.
- Code obfuscation techniques were detected for the app.
- Obfuscation levels are rated as LOW, MEDIUM, ABOVE MEDIUM, HIGH or UNKNOWN. The detected obfuscation level of HIGH provides sophisticated protection against manual analysis which requires a high effort and deep knowledge to reverse the functionality of the app.
- Device administration features not used.
- Application reads out different unique device Ids. These unique identifiers allows to identify the device and to distinguish it from other devices. Another option for reading out these IDs allow to determine the environment. The application can determine if it is running on a real device or on a virtual/emulated device.

- Accessed unique identifier(s): `build model`, `build manufacturer`, `build product`, `build hardware`, `build display`, `build fingerprint`, `build brand`, `IMEI/MEID`, `Wifi-MAC address`, `country code + mobile network code for SIM provider`, `unique Android ID`
- Indicators for usage of advertisement/tracking framework were found.
- The application contains components (Activities) which are exported. This means these parts of the application are accessible or executable by other applications. An external app can write or read information/data to or from this app. Additionally components of this application can be executed. Following Activities are exported:
  - `de.wetteronline.wetterapp.widget.WidgetSnippetConfigure`
  - `de.wetteronline.wetterapp.widget.WidgetConfigure`
  - `com.facebook.CustomTabActivity`
  - `de.wetteronline.wetterapp.MainActivity`
- In this application the allow backup option is enabled. This means the application and all application data will be included when performing a device backup. In case the application contains sensitive information these can be extracted from the backup archive or cloned onto other devices.
- Logging statements found in app. This might leak security or privacy relevant information.
- Permission READ-CONTACTS not used.
- In this application full remote auto backup is enabled. There will be a remote backup of specified, possibly sensitive application data like database entries. The backup will be stored in the Google Cloud. The application defines the whitelisting of files in the backup configuration. The following specified files in the whitelisting will will be remotely stored in the Google Cloud:
  - database:WetterApp2.db
  - `sharedpref:de.wetteronline.wetterapp_preferences.xml`
  - `sharedpref:de.wetteronline.wetterapppro_preferences.xml`
  - sharedpref:Einstellungen.xml
  - sharedpref:MainActivity.xml

  - sharedpref:PREFERENCES.xml

- Application reads information from different sensors. This allows the application to track the user and/or determine the environment of the user.
- World readable/writable preference files detected which can be read/written by other applications.
  - WORLD-READABLE

Runtime Security

- The application contains a registered scheduled alarm. With such an alarm the application repeats the execution of the registered task for example every 10 hours. The following classes register scheduled tasks:
  - `de.wetteronline.lib.wetterapp.background.BackgroundReceiver`
  - `de.wetteronline.wetterapp.widget.a`
- The scheduled task gets repeated in the following intervals:
  - 1 minutes
  - 15 minutes
- The alarm manager has been initialized properly.
- Indicators found for dynamic code loading. The application loads executable code during runtime from a local or external source.
- Android dalvik code is loaded dynamically by the listed methods.
- In the AndroidManifest.xml file the debuggable option is disabled. This prevents some attempts for debugging the application over the adb debug bridge with jdb. Depending of the used Android operating system this flag is not mandatory, in custom ROMs or rooted devices the OS may ignore this flag. On a non stock Android ROM this can still be misused for dynamic analyzes of the application or for doing runtime manipulation. This option should be disabled in released applications.
- The Application has the permission to start automatically after booting the device. The application can execute code without userinteraction or prevention.

Test Performance

- Execution time of all tests: 0:00:46.914

3.20 Wetter.Weather (Android)

3.20.1 Tests

The following Table 3.21 summarizes the results of the Android app `Wetter.Weather` with version *1.4.12*.

Table 3.21: Overview of summarized test results for »Wetter.Weather«

App risks for enterprise usage	
☒	*Implementation flaws? Yes.*
☒	*Privacy risks? Yes.*
☒	*Security risks? Yes.*
Blacklisted by policy	
☒	*Violations of default policy? Yes.*
Communication security	
☒	*Client communication used? Yes.*
☑	*Communication endpoints: 61 entries, see details.*
☑	*Communication with country: 9 entries, see details.*
☒	*SSL/TLS used? Yes.*
☑	*Domains accessed with http AND https:* `play.google.com`
☒	*Custom SSL/TLS trust manager implemented? Yes.*
☐	*Faulty custom SSL/TLS trust manager implemented? No.*
☒	*SSL/TLS using custom error handling? Yes.*
☐	*SSL/TLS using faulty custom error handling? No.*
☐	*SSL/TLS using manual domain name verification? No.*
☒	*Unprotected HTML? Yes.*
☒	*Unprotected JavaScripts? Yes.*
☒	*Unprotected communication? Yes.*
Data security	
☑	*Cryptographic Primitives: 6 entries, see details.*
☒	*Cryptographic keys found? Yes.*
☒	*Constant initialization vectors found? Yes.*
☒	*Application needs normal permissions? Yes.*
☒	*Application needs dangerous permissions? Yes.*
☒	*Application needs system/signature permissions? Yes.*
☑	*Userdefined permission usage: 8 entries, see details.*
☑	*Overprivileged permissions: 13 entries, see details.*
☒	*Is application overprivileged? Yes.*
☒	*Application defines content provider? Yes.*
−	*Content provider accessible without permission: None.*
☒	*JavaScript to SDK API bridge usage? Yes.*
☐	*WiFi-Direct enabled? No.*
Input interface security	

☐	*App can handle documents of mimeType: None.*
☐	*Screenshot protection used? No.*
☐	*Tap Jacking Protection used? No.*

Privacy

☒	*Installed app list accessed? Yes.*
☒	*Obfuscation used? Yes.*
☑	*Obfuscation level is:* `HIGH`
☐	*Device administration policy entries: None.*
☑	*Accessed unique identifier(s): 10 entries, see details.*
☑	*Advertisment-/tracking frameworks found:* `Crashlytics`, `Doubleclick`, `Flurry`, `LiveRail`
☒	*App provides public accessible activities? Yes.*
☒	*Backup of app is allowed? Yes.*
☒	*Log Statement Enabled? Yes.*
☐	*Permission to access address book? No.*
☑	*Sensor usage:* `Camera (inactive)`, `WIFI-Based Location`, `GPS Location`, `Acceleration/Light`
☒	*Unprotected files found? Yes.*
☒	*Unprotected preference files found? Yes.*

Runtime Security

☒	*Scheduled Alarm Manager registered? Yes.*
☑	*Alarm repeating types:* `RTC`, `RTC-WAKEUP`
☒	*Alarm intervals dynamically? Yes.*
☐	*Alarm Manager initialized dynamically? No.*
☒	*Dynamically loaded code at runtime? Yes.*
☑	*Dynamically loaded code at runtime type(s):* `dalvik.system.DexClassLoader(...)`, `ClassLoader.loadClass(...)`, `loadLibrary(...)`
☐	*Allow app debugging Flag? No.*
☒	*Contains native libraries: Yes.*
☑	*Executed component after Phone Reboot:* `com.fotoable.locker.receiver.BootCompletedReceiver`, `com.fotoable.autowakeup.FotoIntentReciver`

3.20.2 Details

The following sections describe details about the test results of `Wetter.Weather` with version *1.4.12*.

App risks for enterprise usage

- Reasons for category implementation flaws:

  - Possible flaw: unintended use of insecure HTTP protocol for transmissions of parameters to servers capable of HTTPS.

- Reasons for category privacy risks:

  - App Listing: Usage of detected functionality to access list of installed apps poses a privacy risk for detected app type.

- Reasons for category security risks:

  - Unprotected Web Content: App loads active web content (e.g. JavaScript or HTML files) without integrity protection. This poses a risk as man-in-the-middle attackers can modify the loaded web content and change the functionality of the app.
  - Crypto: Embedded static encryption key found, which can be extracted by attackers to revert the encryption or fake the signature of the content it is used for.
  - Crypto: Constant initialization vector detected. This should be avoided, as it allows an attacker to infer relationships between segments of encrypted messages if encrypted with the same key and initialization vector.
  - Crypto: Overall quality of cryptographic implementation aspects is rated poor and should be inspected in detail.

Blacklisted by policy

- Reasons for category violations of default policy:

  - Estimated overall app risk for the enterprise exceeds the security policy threshold due to detected risks and flaws exploitable by skilled attackers without the existence of additional supporting factors.

Communication security

- Client communication detected. The application can establish a network connection to one or more specific host systems. URLs with parameters found:

  - `http://cba.trafficmanager.net/materialsv2/conf/?country=`
  - `http://cba.trafficmanager.net/materialsv2/index/?country=`
  - `http://cba.trafficmanager.net/materialsv2/url/?country=`

  - http://play.google.com/store/apps/details?id=com.facebook.orca
  - https://%s/yhs/mobile/search?hspart=cheetah&hsimp=yhs-cheetah_055&type=%s&p=%s
  - https://fonts.googleapis.com/css?family=Oswald:400,700,300
  - https://fonts.googleapis.com/css?family=Roboto:400,700,500,400italic,500italic,700italic
  - https://play.google.com/store/apps/details?id=
  - https://search.yahoo.com/yhs/mobile/search?p=
  - market://details?id=
  - market://details?id=%s
  - market://details?id=com.facebook.orca
  - newsrepublic://news?contentid=

- Communication endpoints is a list of all potential communication endpoints Appicaptor was able to detect. This allows quick enumeration of suspicious domains, raw IP Addresses, etc..
- Communication endpoints: .facebook.com, ab.trafficmanager.net, accuwxturbo.accu-weather.com, ad.cmcm.com, ad6.%s.liverail.com, ad6.liverail.com, api.map.baidu.com, api.mobula.sdk.duapps.com, api.mylnikov.org, api.openweathermap.org, cba.trafficmanager.net, cdn.cmsapi.fotoable.net, cdn.pianoadapi.fotoable.net, cdn.ravenjs.com, cr.m.ksmobile.com, cr.m.liebao.cn, csi.gstatic.com, data.flurry.com, dl.cm.ksmobile.com, dl.fotoable.net, facebook.com, fonts.googleapis.com, geoip.fotoable.com, geoip.fotoable.net, googleads.g.doubleclick.net, goweatherex.3g.cn, graph-video.%s, graph.%s, graph.%s.facebook.com, graph.facebook.com, imgcdn.fotoable.net, itsdata.map.baidu.com, loc.map.baidu.com, maps.owm.io, ms.cmcm.com, music-download.fotoable.net, n.m.ksmobile.net, openweathermap.org, pagead2.googlesyndication.com, pianoaddev.cloudapp.net, play.google.com, proton.flurry.com, rts.mobula.sdk.duapps.com, sb-ssl.google.com, search.yahoo.com, sentry.owm.

io, ssdk.adkmob.com, test.cr.m.ksmobile.com, ud.adkmob.com, ufs.adkmob.com, unconf.adkmob.com, unconf.mobad.ijinshan.com, unrcv.adkmob.com, ups.ksmobile.net, urbica.co, ws.ksmobile.net, www.%s.facebook.com, www.facebook.com, www.fotoable.com, www.googleapis.com, \protect \T1\textbraceleft s\protect \T1\textbraceright .maps.owm.io

- App communicates with servers in 9 countries.
- Communication with country: Austria, Netherlands, Singapore, Hong Kong, United States, China, Ireland, Germany, unknown
- Usage of SSL/TLS can protect the App's communication from adversaries. Tests indicate that communication is at least partly protected with SSL/TLS.
- Mixed usage of HTTP and HTTPS: Protected and unprotected submission of parameters to the same domain. Indicates implementation flaw or weak communication protection.
- Modifications of trust management found. Interface X509TrustManager is implemented or extended.
- Modifications of the SSL error handling detected: Class WebViewClient is extended and onReceivedSslError(...) is overwritten.
- The app loads the following HTML files via unprotected communication (http), which can be exploited by attackers to remotely change the displayed content and functionality of the app:
  - http://music-download.fotoable.net/open/weather/timezoneId
  - http://rts.mobula.sdk.duapps.com/orts/rpb?
  - http://loc.map.baidu.com/iofd.php
  - http://unconf.mobad.ijinshan.com/b/
  - http://ufs.adkmob.com/p/
  - http://api.mobula.sdk.duapps.com/adunion/rtb/getInmobiAd?
  - http://cdn.cmsapi.fotoable.net/screen/category
  - http://n.m.ksmobile.net/news/report
  - http://cr.m.liebao.cn/news/report

- http://goweatherex.3g.cn/goweatherex/city/search
- http://loc.map.baidu.com/tcu.php
- http://unrcv.adkmob.com/rp/
- http://cba.trafficmanager.net/materialsv2/index/?country=
- http://cba.trafficmanager.net/materialsv2/conf/?country=
- http://api.mobula.sdk.duapps.com/adunion/slot/getDlAd?
- http://play.google.com/store/apps/details
- http://cdn.cmsapi.fotoable.net/weather/zodiac
- http://music-download.fotoable.net/open/weather/aqi
- http://www.fotoable.com/privacy.html
- http://cr.m.ksmobile.com/news/report
- http://test.cr.m.ksmobile.com/news/report
- http://loc.map.baidu.com/cc.php
- http://66df88eb63e94f27964b84031e49b358@sentry.owm.io/16
- http://loc.map.baidu.com/sdk_ep.php
- http://cdn.cmsapi.fotoable.net/screen/lists
- http://loc.map.baidu.com/oqur.php
- http://cdn.cmsapi.fotoable.net/weather/horoscope
- http://cba.trafficmanager.net/materialsv2/url/?country=
- http://ud.adkmob.com/r/?
- http://loc.map.baidu.com/wloc
- http://api.mobula.sdk.duapps.com/adunion/slot/getSrcPrio?
- http://music-download.fotoable.net/open/versionCheck

  - http://rts.mobula.sdk.duapps.com/orts/rp?
  - http://accuwxturbo.accu-weather.com/widget/htc2/
  - http://loc.map.baidu.com/user_err.php
  - http://api.mobula.sdk.duapps.com/adunion/rtb/fetchAd?
  - http://loc.map.baidu.com/sdk.php
  - http://itsdata.map.baidu.com/long-conn-gps/sdk.php
  - http://loc.map.baidu.com/rtbu.php
  - http://unconf.adkmob.com/b/

- The app loads the following JavaScript files via unprotected communication (http), which can be exploited by attackers to remotely change the displayed content and functionality of the app:
  - http://openweathermap.org/themes/openweathermap/assets/js/bundle_weathermap.js
  - http://openweathermap.org/themes/openweathermap/assets/js/bundle.js
- The unprotected communication of the App via http connections can be eavesdroped or maliciously modified.
  - http://cba.trafficmanager.net/materialsv2/conf/?country=
  - http://cba.trafficmanager.net/materialsv2/index/?country=
  - http://cba.trafficmanager.net/materialsv2/url/?country=
  - http://play.google.com/store/apps/details?id=com.facebook.orca

Data security

- ECB mode usage identified. This mode has the disadvantage, that identical plaintext blocks are encrypted into identical ciphertext blocks. Therefore it does not hide patterns well and this mode is not recommended for use in cryptographic protocols at all.

- Cryptographic Primitives: "AES/CBC/NoPadding", "AES/CBC/PKCS5Padding", "AES/ECB/PKCS7Padding", "DES/ECB/PKCS5Padding", "DES/ECB/PKCS7Padding", "RSA/ECB/PKCS1Padding"
- It is considered as a bad practice to use hard-coded cryptographic keys in the application. The following hard-coded cryptographic keys were found:
  - "30212102dicudiab"
  - "8a1n9d0i3c1y0c2f"
- Use of constant initialization vectors is a bad practice. The following initialization vectors were found:
  - "30212102dicudiab"
  - "8a1n9d0i3c1y0c2f"
  - 0
- The application requires the following permissions from the protection-level: NORMAL
  - KILL-BACKGROUND-PROCESSES (Allows an application to call android.app.ActivityManager killBackgroundProcesses.)
  - BROADCAST-STICKY (Allows an application to broadcast sticky intents. These are broadcasts whose data is held by the system after being finished, so that clients can quickly retrieve that data without havingto wait for the next broadcast.)
  - READ-EXTERNAL-STORAGE (Allows an application to read from external storage. Any app that declares the WRITE-EXTERNAL-STORAGE permission is implicitly granted this permission. Currently, this permission is not enforced and all apps still have access to read from external storage without this permission. That will change in a future release and apps will require this permission to read from external storage. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
  - VIBRATE (Allows access to the vibrator.)
  - WRITE-SETTINGS (Allows an application to read or write the system settings.)
  - FLASHLIGHT (Allows access to the flashlight.)

  - RECEIVE-BOOT-COMPLETED (Allows an application to receive the android.content.Intent ACTION-BOOT-COMPLETED that is broadcast after the system finishes booting. If you don't request this permission, you will not receive the broadcast at that time. Though holding this permission does not have any security implications, it can have a negative impact on the user experience by increasing the amount of time it takes the system to start and allowing applications to have themselves running without the user being aware of them. As such, you must explicitly declare your use of this facility to make that visible to the user.)
  - WAKE-LOCK (Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming.)
  - EXPAND-STATUS-BAR (Allows an application to expand or collapse the status bar.)
  - ACCESS-WIFI-STATE (Allows applications to access information about Wi-Fi networks)
  - CHANGE-NETWORK-STATE (Allows applications to change network connectivity state.)
  - ACCESS-NETWORK-STATE (Allows applications to access information about networks.)

- The application requires the following permissions from the protection-level: DANGEROUS
  - WRITE-EXTERNAL-STORAGE (Allows an application to write to external storage. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)
  - CHANGE-WIFI-STATE (Allows applications to change Wi-Fi connectivity state.)
  - INTERNET (Allows applications to open network sockets.)
  - PROCESS-OUTGOING-CALLS (Allows an application to monitor, modify, or abort outgoing calls.)
  - ACCESS-FINE-LOCATION (Allows an app to access precise location from location sources such as GPS, cell towers, and Wi-Fi.)
  - DISABLE-KEYGUARD (Allows applications to disable the keyguard.)
  - READ-PHONE-STATE (Allows read only access to phone state. Note: If both minSdkVersion and targetSdkVersion values are set to 3 or lower, the system implicitly grants this permission to the app.)

  - SYSTEM-ALERT-WINDOW (Allows an application to open windows using the type android.view.WindowManager.LayoutParams TYPE-SYSTEM-ALERT, shown on top of all other applications. Very few applications should use this permission. these windows are intended for system-level interaction with the user.)
  - ACCESS-COARSE-LOCATION (Allows an app to access approximate location derived from network location sources such as cell towers and Wi-Fi.)
  - BLUETOOTH-ADMIN (Allows applications to discover and pair bluetooth devices.)
  - GET-TASKS (Allows an application to get information about the currently or recently running tasks.)
  - BLUETOOTH (Allows applications to connect to paired Bluetooth devices.)

- The application requires the following permissions from the protection-level: DANGEROUS
  - BIND-ACCESSIBILITY-SERVICE (Must be required by an android.accessibilityservice.AccessibilityService, to ensure that only the system can bind to it.)
  - BIND-NOTIFICATION-LISTENER-SERVICE (Must be required by an android.service.notification.NotificationListenerService, to ensure that only the system can bind to it.)
  - MODIFY-PHONE-STATE (Allows modification of the telephony state - power on, mmi, etc. Does not include placing calls. Not for use by third-party applications.)
  - MOUNT-UNMOUNT-FILESYSTEMS (Allows mounting and unmounting file systems for removable storage. Not for use by third-party applications.)
  - PACKAGE-USAGE-STATS (Allows an application to collect component usage statistics.)
  - WRITE-APN-SETTINGS (Allows applications to write the APN settings. Not for use by third-party applications.)

- Application uses userdefined permissions. Application can access data of a foreign application which requires this permission to access data.
- Userdefined permission usage: `android.alarm.permission.SET-ALARM`, `android.permission.SYSTEM-OVERLAY-WINDOW`, `com.android.launcher.permission.UNINSTALL-SHORTCUT`, `com.android.launcher.permission.INSTALL-SHORTCUT`, `com.google.android.`

providers.gsf.permission.READ-GSERVICES, com.android.launcher.permission.READ-SETTINGS, com.android.vending.BILLING, com.google.android.gms.permission.ACTIVITY-RECOGNITION

- Overprivileged permissions: FLASHLIGHT, MODIFY-PHONE-STATE, EXPAND-STATUS-BAR, SYSTEM-ALERT-WINDOW, PROCESS-OUTGOING-CALLS, WRITE-APN-SETTINGS, BIND-NOTIFICATION-LISTENER-SERVICE, PACKAGE-USAGE-STATS, MOUNT-UNMOUNT-FILESYSTEMS, BIND-ACCESSIBILITY-SERVICE, BROADCAST-STICKY, CHANGE-NETWORK-STATE, READ-EXTERNAL-STORAGE
- Application is propably overprivileged. Application has too much permissions. Foreign applications may be able to abuse this permission.
- The application uses a content provider for interacting with data set structures. Content providers are the standard interface that connects data in one process with code running in another process.
- Every ContentProvider defined in the application is protected by a permission. To access the interface from an external application it must request access to it. The interface is only available if an application defines these permissions.
- Indicator for JavaScript bridge to Android API usage found. JavaScript used in the application (localy stored or loaded dynamicaly) may access and execute Android SDK API calls.
- Wifi-Direct is not enabled. There is no risk for exploiting a vulnerability in the wpa-supplicant module responsible for the wlan management. (http://www.coresecurity.com/advisories/android-wifi-direct-denial-service)

Input interface security

- No indicators for file handling found. The app does not define a filter scheme to process specific files.
- The app does not use protection measures for preventing screenshots. For apps displaying sensitive data it is recommended to disable screenshots.
- The application is vulnerable to tapjacking. When the protection is not used inside an exported activity another application is able to redirect touch events to the exported activity without the users consent.

Privacy

- The Application gathers a list of installed applications. Even though some legitimate applications may use this functionality, it can be misused to send this information to third parties.

- Code obfuscation techniques were detected for the app.
- Obfuscation levels are rated as LOW, MEDIUM, ABOVE MEDIUM, HIGH or UNKNOWN. The detected obfuscation level of HIGH provides sophisticated protection against manual analysis which requires a high effort and deep knowledge to reverse the functionality of the app.
- Device administration features not used.
- Application reads out different unique device Ids. These unique identifiers allows to identify the device and to distinguish it from other devices. Another option for reading out these IDs allow to determine the environment. The application can determine if it is running on a real device or on a virtual/emulated device.
- Accessed unique identifier(s): `build model`, `build manufacturer`, `build product`, `build display`, `build brand`, `IMEI/MEID`, `subscriber ID (IMSI)`, `Wifi-MAC address`, `country code + mobile network code for SIM provider`, `unique Android ID`
- Indicators for usage of advertisement/tracking framework were found.
- The application contains components (Activities) which are exported. This means these parts of the application are accessible or executable by other applications. An external app can write or read information/data to or from this app. Additionally components of this application can be executed. Following Activities are exported:
  - `com.cmcm.newssdk.ui.NewsWebViewDetailActivity`
  - `com.cmcm.newssdk.ui.NewsOnePageDetailActivity`
  - `com.facebook.CustomTabActivity`
  - `com.fotoable.weather.view.acitivity.AlarmClockActivity`
  - `com.fotoable.weather.view.acitivity.NewsActivity`
- In this application the allow backup option is enabled. This means the application and all application data will be included when performing a device backup. In case the application contains sensitive information these can be extracted from the backup archive or cloned onto other devices.
- Logging statements found in app. This might leak security or privacy relevant information.
- Permission READ-CONTACTS not used.

- Application reads information from different Sensors. This allows the application to track the user and/or determine the environment of the user. There was no Permission defined for camera usage, but the application contains specific API calls accessing the camera.Missing permissions despite of API calls could be an indication for missconfiguration or plugin/library code which is not used. For more detailed information application has to be reviewed manually.
- World readable/writable files detected which can be read/written by other applications.
  - WORLD-READABLE
- World readable/writable preference files detected which can be read/written by other applications.
  - WORLD-READABLE

Runtime Security

- The application contains a registered scheduled alarm. With such an alarm the application repeats the execution of the registered task for example every 10 hours. The following classes register scheduled tasks:
  - `com.daemon.keepalive.KeepAliveService`
  - `com.fotoable.weather.receiver.PeriodicRefreshReceiver`
  - `com.cmcm.adsdk.b.a`
- The scheduled task gets repeated in the following intervals:
  - 2 hours
  - Dynamic interval(s)
- The alarm manager has been initialized properly.
- Indicators found for dynamic code loading. The application loads executable code during runtime from a local or external source.
- Android dalvik code is loaded dynamically by the listed methods. Native code by Java Native Interface (for dynamic loading) is used.
- In the AndroidManifest.xml file the debuggable option is disabled. This prevents some attempts for debugging the application over the adb debug bridge with jdb. Depending of the used Android operating system this flag is not mandatory, in custom ROMs or rooted devices the OS may ignore this flag. On a non stock Android ROM this can still be misused for dynamic analyzes of the application or for doing runtime manipulation. This option should be disabled in released applications.

- Loadable libraries found:
  - ARMv8 64 bit: lib/arm64-v8a/liblocSDK7.so
  - ARMv8 64 bit: lib/arm64-v8a/liblocalpushservice.so
  - ARM 32 bit: lib/armeabi-v7a/liblocSDK7.so
  - ARM 32 bit: lib/armeabi-v7a/liblocalpushservice.so
  - ARM 32 bit: lib/armeabi/liblocSDK7.so
  - ARM 32 bit: lib/armeabi/liblocalpushservice.so
  - x86 32bit: lib/x86/liblocSDK7.so
  - x86 32bit: lib/x86/liblocalpushservice.so
  - x86 64bit: lib/x86_64/liblocSDK7.so
  - x86 64bit: lib/x86_64/liblocalpushservice.so
- The Application has the permission to start automatically after booting the device. The application can execute code without userinteraction or prevention.

Test Performance

- Execution time of all tests: 0:01:14.298

4 Glossary

3DES

Triple DES or 3DES is the common name for the Triple Data Encryption Algorithm (TDEA or Triple DEA) symmetric-key block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block. The original DES cipher's key size of 56 bits was generally sufficient when that algorithm was designed, but the availability of increasing computational power made brute-force attacks feasible.
URL: `http://en.wikipedia.org/wiki/Triple_DES`

Address book

All sorts of information about a person can be stored within the global address book including email addresses, phone numbers, addresses, websites, chat names, and more. Apps can access the address book based on different requirements or methods (Android: permission based, iOS: access with user interaction or direct access without user interaction (deprecated)). Appicaptor evaluates the methods and API function calls of address book access as well as their context (e.g. user interaction, permission analysis)
URL: `http://developer.android.com/reference/android/Manifest.permission.html#READ_CONTACTS`, `https://developer.apple.com/library/ios/documentation/ContactData/Conceptual/AddressBookProgrammingGuideforiPhone/Introduction.html`

Advertisement frameworks

Appicaptor evaluates different advertisement and tracking frameworks e.g., Apple ID Support for Ads, Google AdMob, Apple iAd, OpenUDID, Google Analytics, possibly other AD/-Tracking, MillennialMedia, mopub, MobClix, TapJoy, Flurry, inMobi AD Tracker, MobFox, mdotm, AdWhirl, Crashlytics, inneractive, AdFonic, Mocean Mobile, GreyStripe, inMobi ADs, RevMob Ads, AdMarvel, Madvertise, Crittercism, Adobe Omniture Tracker, Burstly, Jumptap, Urban Airship, Unity3D. Advertisement frameworks grant apps access to identifiers that can be used for serving advertisements or ad tracking.

Content provider (Android)
Content providers manage access to a structured set of data. They encapsulate the data, and provide mechanisms for defining data security. Content providers are the standard interface that connects data in one process with code running in another process. As content providers are one potential way to leak data to other apps Appicaptor searches for content provider creation in apps.
URL: `http://developer.android.com/guide/topics/providers/content-providers.html`

AES
Advanced Encryption Standard (AES) is the standard symmetric-key block encryption algorithm with a block size of 128 bits and encryption key length of 128, 192 or 256 bits.
URL: `http://en.wikipedia.org/wiki/Advanced_Encryption_Standard`

ARC (iOS)
see Automatic reference counting (ARC)

ASLR-PIE (iOS)
Address space layout randomization (ASLR) protects apps from buffer overflow attacks. In order to prevent an attacker from reliably jumping to a particular exploited function in memory, ASLR involves randomly arranging the positions of key data areas of a program, including the base of the executable and the positions of the stack, heap, and libraries, in a process's address space. For full ASLR protection, the app has to be compiled with support for PIE (position-independent executable). Appicaptor evaluates whether or not the ASLR-PIE compile option was set during app creation.
URL: `http://en.wikipedia.org/wiki/Address_space_layout_randomization`, `https://developer.apple.com/library/ios/qa/qa1788/_index.html`

Automatic reference counting (ARC)
(iOS)

In Objective-C programming, Automatic Reference Counting (ARC) is a memory management enhancement where the burden of keeping track of an object's reference count is lifted from the programmer to the compiler. In traditional Objective-C, the programmer would send retain and release messages to objects in order to mark objects for deallocation or to prevent deallocation. Under ARC, the compiler does this automatically by examining the source code and then adding the retain and release messages in the compiled code.Appicaptor evaluates whether or not the ARC compile option was set during app deployment.
URL: `http://en.wikipedia.org/wiki/Automatic_Reference_Counting`, `https://developer.apple.com/library/ios/releasenotes/ObjectiveC/RN-TransitioningToARC/Introduction/Introduction.html`

Background activities

If the user performs an action that starts another app or switches to another app, the operating system moves the previously running app into the background (where the activity is no longer visible, but the instance and its state remains intact). Appicaptor evaluates the methods and API function calls of iOS background modes for audio (play and record audible content in background), location (provide location-based information to the user), voip (provide Voice-over-IP services and automatically launch after system boot so that the app can reestablish VoIP services (and is allowed to play and record background audio)), newsstand-content (process content that was recently downloaded in the background using the Newsstand Kit framework), external-accessory (communicate with an accessory that delivers data at regular intervals), bluetooth-central (use the Core-Bluetooth framework to communicate with a Bluetooth accessory while in the background), bluetooth-peripheral (use the CoreBluetooth framework to communicate in peripheral mode with a Bluetooth accessory), remote-notification (use remote notifications to resume or launch the app in the background for downloading new content), fetch (request a launch or resume by the system to fetch new content from the network on a regular basis).
URL: `https://developer.apple.com/library/ios/#documentation/general/Reference/InfoPlistKeyReference/Articles/iPhoneOSKeys.html#//apple_ref/doc/uid/TP40009252-SW22`

Blacklist Application blacklisting is a common administration practice to prevent the execution of undesirable programs. Such programs may include apps known to contain security threats or vulnerabilities but also those that are deemed inappropriate within an organization. Appicaptor will mark an app as blacklisted when Appicaptor findings are not compliant to your policy rule set.

CAST CAST is a symmetric-key block cipher with a block size of 64 bits and encryption key length of 40 to 128 bits. It is used in a number of products, notably as the default cipher in some versions of GPG and PGP.
URL: `http://en.wikipedia.org/wiki/CAST-128`

CBC In Cipher-block chaining (CBC) mode, each block of plaintext is XORed with the previous ciphertext block before being encrypted. This way, each ciphertext block depends on all plaintext blocks processed up to that point. To make each message unique, an initialization vector must be used in the first block.
URL: `http://en.wikipedia.org/wiki/Block_cipher_mode_of_operation`

Client communication The client–server model of computing is a distributed application structure that partitions tasks or workloads between the providers of a resource or service, called servers, and service requesters, called clients. Often clients and servers communicate over a computer network on separate hardware. A server host runs one or more server programs which share their resources with clients. A client requests a server's content or service function and therefore initiate communication sessions with servers which await incoming requests. Appicaptor evaluates the methods and API function calls that initiate, perform and end communication processes with external entities.
URL: `http://en.wikipedia.org/wiki/Client%E2%80%93server_model`

Communication security Secure communication is achieved when two entities are communicating in a way not susceptible to eavesdropping, interception and manipulation. Appicaptor validates the communication security characteristics in terms of correct communication counterpart authenticity check implementations, and communication protection characteristics (integrity and encryption).
URL: `http://en.wikipedia.org/wiki/Secure_communication`

Compiler Flags The compiler transforms source code written in a programming language into another computer language (the target language, often resulting in a binary form known as object code). Several compile-time options can be used to help hardening a resulting binary e.g., against memory corruption attacks. Appicaptor evaluates the compile-time options applied during app deployment.

Custom SSL/TLS trust manager See SSL Trust Management Modification

Data Protection Data at rest on the mobile device is subject to multiple threats. To prevent this data from being unauthorizedly accessed, modified or stolen, mobile operating systems employ security protection measures such as password protection, data encryption, or a combination of both.

Data Protection (iOS) Data protection is available for iOS devices that offer hardware encryption, including iPhone 3GS and later, all iPad models, and iPod touch (3rd generation and later). Data protection enhances the built-in hardware encryption by protecting the hardware encryption keys with the device passcode. This provides an additional layer of protection for specific data on rest. Especially if a device is lost.
URL: `http://support.apple.com/kb/ht4175`

Data protection classes (iOS) When a new file is created on an iOS device, it is assigned to a specific class by the app that creates it or the default class is utilized when no specific class is assigned. The default class is NSFileProtectionComplete when an app was installed on iOS 7 whereas it is NSFileProtectionNone when an app was installed on iOS6 or prior. Each class uses different policies to determine when the data is accessible. The basic classes and policies are as follows: complete protection (NSFileProtectionComplete), protected unless open (NSFileProtectionCompleteUnlessOpen), protected until first user authentication (NSFileProtectionCompleteUntilFirstUserAuthentication) and no protection (NSFileProtectionNone). Appicaptor evaluates all file generation and modification processes within the evaluated app and monitors the (default) assignment of data protection classes to these files.
URL: `https://www.apple.com/privacy/docs/iOS_Security_Guide_Oct_2014.pdf`

Data security Appicaptor evaluates different aspects of data security: data protection (data on rest protection, see data protection), permission analysis, etc.

Default trust anchor

DES	The Data Encryption Standard (DES) is an outdated symmetric-key encryption algorithm which is now considered to be insecure for many applications. URL: `http://en.wikipedia.org/wiki/Data_Encryption_Standard`
Document types	If an app is capable of opening specific types of files, the app may indicate that support to the operating system. This allows other apps to offer the user the option to hand off those files to that mentioned app. Appicaptor extracts all document types an app can handle. URL: `https://developer.apple.com/library/ios/Documentation/FileManagement/Conceptual/DocumentInteraction_TopicsForIOS/Articles/RegisteringtheFileTypesYourAppSupports.html` , `http://developer.android.com/reference/android/content/Intent.html`
Domains accessed with HTTP and HTTPS	See Mixed usage of HTTP and HTTPS
Dynamically loaded code (Android)	Loading (external) executable code while an app is running.
ECB	The simplest of the encryption modes of a block cipher algorithm is the electronic codebook (ECB) mode. The message is divided into blocks, and each block is encrypted separately. URL: `http://en.wikipedia.org/wiki/Block_cipher_mode_of_operation`
Flaw	A software flaw is an error, failure, or fault in a computer program or system that causes it to produce an incorrect or unexpected result, or to behave in unintended ways.
fstack-protector-all (iOS)	iOS applications can apply stack smashing protection at compile time. This can be achieved by specifying the compiler option named fstack-protector-all

iCloud Usage iCloud is a cloud storage and cloud computing service provided by Apple. It allows data syncing for email, contacts, calendars, bookmarks, notes, reminders (to-do lists), iWork documents, photos and other data. The service also allows users to wirelessly back up their iOS devices to iCloud. Appicaptor examines iCloud usage as an option to store private or sensitive data with potentially different protection measures than the app's selected protection measures on the mobile device.
URL: `https://www.icloud.com/`

Implementation flaw See flaw

InApp purchase In-App purchase in apps enables the app developer to sell content or features directly within a free or paid app, e.g., premium content, virtual goods, or subscriptions.

JavaScript to SDK API bridge (Android) WebViews JavaScript API Calls to all Android Java methods are possible in case the app is executed on Android before 4.2 (remote code injection)
URL: `http://developer.android.com/reference/android/webkit/WebView.html#addJavascriptInterface%28java.lang.Object,%20java.lang.String%29`, `http://sseblog.ec-spride.de/2013/09/java-script-attack-vector/`

Keychain (iOS) Apps need to handle passwords and other sensitive data, such as keys or tokens. The iOS keychain provides a way to store these items. Rather than limiting access to a single process or app, access groups allow keychain items to be shared between apps. Keychain items can only be shared between apps from the same developer.
URL: `https://www.apple.com/privacy/docs/iOS_Security_Guide_Oct_2014.pdf`

Keychain classes (iOS)
The basic classes are as follows: Access to keychain entries when device is unlocked (kSecAttrAccessibleWhenUnlocked), after first unlock (kSecAttrAccessibleAfterFirstUnlock) or always (kSecAttrAccessibleAlways). Apps with background refresh services in iOS 7 require the keychain class kSecAttrAccessibleAfterFirstUnlock for keychain items when that information is accessed during background updates. Each keychain class has a "This device only" counterpart, which is always protected with device specific Key (the UID-key) when being copied from the device during a backup, rendering it useless if restored to a different device. Appicaptor evaluates all keychain generation and modification processes within the evaluated app and monitors the assignment of keychain entry classes.
URL: `https://www.apple.com/privacy/docs/iOS_Security_Guide_Oct_2014.pdf`

Log Statement
For e.g., application debugging there is the opportunity to utilize log statements to write data to the global device log. As the usage of log statements is one potential way to leak data Appicaptor searches for the usage of log statements in apps.

Malicious behaviour
Malicious app behavior affects the app user directly e.g. through some action within a malicious app that harms the user's data, information or processes. Malicious actions could be e.g. unauthorized data leakage, data modification or social engineering.

MD5
The MD5 message-digest algorithm is a widely used cryptographic hash function producing a 128-bit (16-byte) hash value. The security of the MD5 hash function is severely compromised, as a collision attack exists that can find collisions within seconds.
URL: `http://en.wikipedia.org/wiki/MD5`

Message UI (iOS)
The Message UI framework provides view controllers for presenting composition interfaces for email and SMS messages within a 3rd party app without requiring the user to leave the app.
URL: `https://developer.apple.com/library/ios/Documentation/MessageUI/Reference/MessageUI_Framework_Reference/_index.html`

Mixed usage of HTTP and HTTPS
When an app transmits data to a server via http that is capable of https the app does not utilize the maximum amount of protection that is offered by its communication counterpart. To detect potential but avoidable information leakage based on unprotected communication Appicaptor searches and documents for http usage when the target server is capable of https communication, as this characteristic is crucial to data in transit protection.

OpenSSL Usage
The OpenSSL Project develops a Open Source toolkit implementing the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols. The project is managed by a worldwide community of volunteers. Appicaptor checks whether or not OpenSSL used within an app.
URL: `https://www.openssl.org/`

Overprivileged
Serveral apps ask for more permissions than necessary (according to their app functionality and utilized API methods within the app). This is because they are integrated with the operating system at a low level by device manufacturers or app developer requests more permissions than required (e.g., within Android app manifest file).

Padding
A block cipher works on units of a fixed size (known as a block size), but messages come in a variety of lengths. So some modes (namely ECB and CBC) require that the final block be padded before encryption. Several padding schemes exist. The simplest is to add null bytes to the plaintext to bring its length up to a multiple of the block size, but care must be taken so that the original length of the plaintext can be recovered. As an example the value of each added byte by PKCS7 padding is the number of bytes that are added.
URL: `http://en.wikipedia.org/wiki/Padding_(cryptography)`

Passbook (iOS)
With Passbook apps can store boarding passes, event tickets, retail coupons, store cards and generic passes. These elements include barcodes that can be scanned in order to convey information stored in the pass to perform actions in the physical world. As the usage of passbook is one potential way to leak data Appicaptor searches for the usage of passbook in apps.
URL: `https://developer.apple.com/passbook/`

Pasteboard Types (iOS)
When the user requests a copy or cut operation on a selection in the user interface an object in the app writes data to a pasteboard. Another object in the same or a different app then reads that data from the pasteboard and presents it to the user at a new location; this usually happens when the user requests a paste operation. The copy and paste actions can be processed with two different apps. To share data with any other app, the app can either use the system-wide pasteboard; or to share data with another app that has the same team ID as the initial app, the app-specific pasteboards can be utilized. As the usage of pasteboards is one potential way to leak data Appicaptor searches for the utilized pasteboard type and the usage of the system-wide pasteboard if available.
URL: `https://developer.apple.com/library/ios/documentation/uikit/reference/UIPasteboard_Class/Reference.html`

Permission (Android)
Android is a privilege-separated operating system, in which each application runs with a distinct system identity (Linux user ID and group ID). Additional finer-grained security features are provided through a "permission" mechanism that enforces restrictions on the specific operations that a particular process can perform, and per-URI permissions for granting ad hoc access to specific pieces of data.
URL: `http://developer.android.com/guide/topics/security/permissions.html`

PIE (iOS)
see ASLR-PIE

Privacy
Data privacy deals with the ability of an organization or individual to restrict the sharing of data with third parties.

Privacy violations
Privacy violations refers to a process in which personal, sensitive information are exposed to unauthorized third parties. Appicaptor detects privacy violations based on e.g., unauthorized screenshot captures, access to device identifiers, address book usage without notification, advertisement-/tracking frameworks usage, sensor usage (location, microphone, camera, etc.), log statements utilized, message UI usage, iCloud usage, Pasteboard or passbook usage, etc.

RC2
RC2 a symmetric-key block cipher with a block size of 64 bits and encryption key length of 8–1024 bits, in steps of 8 bits.
URL: `http://en.wikipedia.org/wiki/RC2`

RC4 Stream cipher used in popular protocols such as Transport Layer Security (TLS) (to protect Internet traffic) and WEP (to secure wireless networks). While remarkable for its simplicity and speed in software, RC4 has weaknesses that argue against its use in new systems.
URL: http://en.wikipedia.org/wiki/RC4

Runtime Security Runtime security summarizes Appicaptor test cases that refer to methods to harden the application binary based on compile-time options as well as the ability to execute dynamically loaded code.

Security violations Security violations refers to a circumstance that a process or data handling is not protected in an appropriate manner.

Sensor usage App's access to smartphone sensors, with or without user interaction. Appicaptor detects access to sensor data such as location data and location updates, microphone, and camera data.

SHA1 The SHA1 message-digest algorithm is a widely used cryptographic hash function producing a 160-bit (20-byte) hash value. Attacks were found on SHA-1 therefore it is recommended to move to SHA-2.
URL: http://en.wikipedia.org/wiki/SHA-1

Social Network usage App's interaction with social networks, based on social network framework or library usage. Appicaptor detects social network interaction with Twitter, Facebook and Weibo.

SSL Secure Sockets Layer (SSL), and its successor Transport Layer Security (TLS), are cryptographic protocols which were designed to provide communication security (integrity, authenticity and confidentiality) over untrusted communication channels.
URL: http://tools.ietf.org/html/rfc6101

SSL Error Handling Modification If using WebViews in coordination with SSL/TLS the app developer can modify the SSLErrorHandler. One intention to do so is to accept self-signed or even all certificates, even incorrect ones. Appicaptor detects and notifies SSL error handling modifications as these open the opportunity to improper SSL error handling and therefore facilitate Man-in-the-Middle attacks.
URL: http://developer.android.com/reference/android/webkit/SslErrorHandler.html

SSL/TLS usage See SSL or TLS

SSL/TLS using custom error handling	See SSL Error Handling Modification
SSL/TLS using faulty custom error handling	This refers also to SSL Error Handling Modification, but in this circumstance there is at least one point of execution where the communication proceeds even if an error is indicated. Appicaptor detects and notifies faulty custom SSL error handling modifications as these open the opportunity to improper SSL error handling and therefore facilitate Man-in-the-Middle attacks.
SSL/TLS using improper certificate validation	The communications security of SSL/TLS bases on the authenticity and integrity of the utilized server certificates. If an app implements a SSL/TLS certificate check itself and does not use the operating system's functions to validate certificates. Faulty checks can render the SSL/TLS usage for communication security useless. Appicaptor detects improper certificate validation as this opens the opportunity for Man-in-the-Middle attacks.
SSL/TLS using manual domain name verification	The ALLOW_ALL HostnameVerifier essentially turns hostname verification off. URL: `http://developer.android.com/reference/org/apache/http/conn/ssl/AllowAllHostnameVerifier.html`
SSL/TLS with changed cipher list	Appicaptor detects wether or not the app implementation changes the default SSL/TLS cipher sets.
stack smashing protection (iOS)	Stack buffer overflows occur when a program writes to a memory address on the program's call stack outside of the intended data structure. The stack smashing protection is a compile-time option to mitigate the effects of stack buffer overflows.
Static passwords in URLs	Some apps transmit certain static credentials in URL parameters. As URL parameters are not protected as they are part of the HTTP header, this is a potential way to unintentionally leak sensitive data.
TLS	Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), is a cryptographic protocol which is designed to provide communication security (integrity and confidentiality) over untrusted communication channels URL: `http://tools.ietf.org/html/rfc2246`, `http://tools.ietf.org/html/rfc4346` , `http://tools.ietf.org/html/rfc5246`

Tracking framework	See Advertisement frameworks
URL schemata	Apps that support custom URL schemes can use those schemes to receive messages. Appicaptor searches if an app registers for these URL schemes to receive external data. URL: `https://developer.apple.com/library/ios/featuredarticles/iPhoneURLScheme_Reference/Introduction/Introduction.html`
Web view	A Web View is an element that displays web pages within apps without starting a dedicated stand alone browser. Appicaptor checks if Web Views are used within apps. URL: `http://developer.android.com/reference/android/webkit/WebView.html` , `https://developer.apple.com/library/ios/documentation/uikit/reference/UIWebView_Class/Reference/Reference.html`