ANDROID STATIC ANALYSIS REPORT

COVID Radar (1.1.2)

File Name:	COVID Radar 1.1.2.apk
Package Name:	nl.lumc.covidradar
Average CVSS Score:	6.3
App Security Score:	10/100 (CRITICAL RISK)
Trackers Detection:	1/285

FILE INFORMATION

File Name: COVID Radar 1.1.2.apk
Size: 5.49MB
MD5: 257005af63479216e6f63f40c17136d4
SHA1: fa800a2cab5286382aa45c9e841c8f53439fe685
SHA256: 982ccb480cd96cb0f5d5e8343297a3787e7e3456b1a07de4e105a57b4e901862

APP INFORMATION

App Name: COVID Radar
Package Name: nl.lumc.covidradar
Main Activity: com.imgzine.androidcore.CoreActivity
Target SDK: 29
Min SDK: 23
Max SDK:
Android Version Name: 1.1.2
Android Version Code: 6

APP COMPONENTS

Activities: 2
Services: 11
Receivers: 12
Providers: 2
Exported Activities: 0
Exported Services: 1
Exported Receivers: 2
Exported Providers: 0

CERTIFICATE INFORMATION

```
APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=NL, ST=NH, L=Amsterdam, O=imgZine, OU=development, CN=Gertjan Smits
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2013-02-21 13:17:24+00:00
Valid To: 2153-04-28 13:17:24+00:00
Issuer: C=NL, ST=NH, L=Amsterdam, O=imgZine, OU=development, CN=Gertjan Smits
Serial Number: 0x51261e64
Hash Algorithm: sha1
md5: 8a6e1e721efc46c8e23f70cc22eb3e54
sha1: 76fccc2fed318941fe973c9967bb8fd13df1d6ee
sha256: a3885f440238818682aa9c43d5e014a4927dff5310ef9e0c5845e39b0c49f442
sha512:
a875ca31ebf388948427bc1081fddd64d4f492b18c3a3e1c73e2d2d7a1cf5cf4a05096bbfa5f5e596cedbe4d8d083fc1072e0722ce7ecbbb741baddc16e3a896
```

PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: fc6755fcca5c1f869f3ec3a11bae13c805a542515d86e63dba338d24de8efdd5

Certificate Status: Warning
Description: The app is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues.The manifest indicates SHA256withRSA is in use. Please verify this manually.

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	dangerous	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete SD card contents	Allows an application to write to the SD card.
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read SD card contents	Allows an application to read from SD Card.
android.permission.WAKE_LOCK	dangerous	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	dangerous	Unknown permission from android reference	Unknown permission from android reference
com.google.android.c2dm.permission.RECEIVE	signature	C2DM permissions	Permission for cloud to device messaging.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check
Build.HARDWARE check
Build.TAGS check</td></tr>
<tr><td>Compiler</td><td>dx</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.imgzine.androidcore.CoreActivity	Schemes: rivmcovid://, https://, Hosts: deep.link, covidradar.nlinzorg.nl, Path Patterns: /start, /a/.*, /s/.*/a/.*, /c/.*, /c/.*/a/.*, /c/.*/s/.*/a/.*, /e/.*, /tab/.*, /newsletter,

MANIFEST ANALYSIS

ISSUE	SEVERITY	DESCRIPTION
Application Data can be Backed up [android:allowBackup=true]	medium	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.

ISSUE	SEVERITY	DESCRIPTION
Broadcast Receiver (com.google.android.gms.measurement.AppMeasurementInstallReferrerReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.INSTALL_PACKAGES [android:exported=true]	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	high	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

CODE ANALYSIS

ISSUE	SEVERITY	STANDARDS	FILES
			c0/l0.java z/w.java z/s.java z/h0.java z/g.java z/u.java z/i0.java z/m.java

ISSUE	SEVERITY	STANDARDS	FILES
			z/a.java z/j0/i/b.java z/j0/h/c.java z/j0/k/b.java z/j0/k/a.java b0/a/e/d.java v/i/f/b/a.java v/i/m/y.java v/i/m/z/c.java v/i/m/z/d.java v/n/d/u.java v/s/o.java v/s/d.java v/f/c.java v/f/h.java v/f/g.java v/a0/q.java v/a0/d0.java v/e0/c.java v/e0/d.java v/e0/e.java v/e0/g.java v/e0/r.java v/e0/v/r/d.java v/e0/v/r/p.java v/e0/v/r/g.java v/e0/v/p/f/b.java v/e0/v/p/f/f.java v/e0/v/p/f/a.java v/c/a/b/b.java v/v/a0/d.java v/q/c.java v/b/q/e0.java v/b/q/n0.java com/imgzine/androidcore/content/tabs/TabJson.java com/imgzine/androidcore/engine/comments/json/ArticleInfoCommentsRequestBody.java com/imgzine/androidcore/engine/comments/json/Comment.java com/imgzine/androidcore/engine/reporter/json/ReporterPostArticle.java com/imgzine/androidcore/engine/reporter/json/ReporterPostRequestBody.java com/imgzine/androidcore/engine/reporter/json/ReporterPostResponse.java com/imgzine/androidcore/engine/user/AppPreferences.java com/imgzine/androidcore/engine/search/json/SearchRequestBody.java com/imgzine/androidcore/engine/search/json/SearchResultArticle.java com/imgzine/androidcore/engine/search/json/SearchResponse.java com/imgzine/androidcore/engine/taxonomy/TaxonomyEntry.java com/imgzine/androidcore/engine/workers/DownloadFileWorker.java com/imgzine/androidcore/engine/profiles/json/Profile.java com/imgzine/androidcore/engine/profiles/json/ProfilesRequestBody.java com/imgzine/androidcore/engine/profiles/json/ProfilesResponse.java

ISSUE	SEVERITY	STANDARDS	FILES
This App uses Java Hash Code. It's a weak hash function and should never be used in Secure Crypto Implementation.	warning	**CVSS V2:** 2.3 (low) **CWE:** CWE-327 - Use of a Broken or Risky Cryptographic Algorithm **OWASP MASVS:** MSTG-CRYPTO-4	com/imgzine/androidcore/engine/timeline/ArticleCollectionSpec.java com/imgzine/androidcore/engine/timeline/ArticleDetail.java com/imgzine/androidcore/engine/timeline/json/ArticleByLinkResponse.java com/imgzine/androidcore/engine/timeline/json/TimelineResponse.java com/imgzine/androidcore/engine/timeline/json/Article.java com/imgzine/androidcore/engine/timeline/json/ArticleDetailResponse.java com/imgzine/androidcore/engine/timeline/json/ArticleCollection.java com/imgzine/androidcore/engine/conf/json/ChannelJson.java com/imgzine/androidcore/engine/conf/json/ChannelChannelJson.java com/imgzine/androidcore/engine/conf/json/SourceJson.java com/imgzine/androidcore/engine/analytics/InboxUpdate.java com/imgzine/androidcore/authentication/internal/login/TokenResponse.java com/imgzine/androidcore/authentication/internal/login/TokenRequestBody.java e/g/a/y.java e/g/a/d0/b.java e/a/a/a/e.java e/a/a/a/l.java e/a/a/a/t/o.java e/a/a/a/a0/c.java e/a/a/a/a0/g.java e/a/a/a/b0/a.java e/a/a/a/p/n.java e/a/a/c/p.java e/a/a/c/i.java e/a/a/c/v0/a.java e/a/a/c/i0/i.java e/a/a/c/i0/f.java e/a/a/c/j0/b/b.java e/a/a/c/j0/b/a.java e/a/a/c/u/b.java e/a/a/c/u/a.java e/a/a/c/a/u.java e/a/a/c/k0/b.java e/a/a/c/k0/c.java e/a/a/c/b0/d/c.java e/a/a/c/b0/d/h.java e/a/a/c/b0/d/d.java e/a/a/c/b0/d/e.java e/a/a/c/b0/d/g.java e/a/a/c/b0/d/a.java e/a/a/c/b0/d/i/b.java e/a/a/c/b0/d/i/c.java e/a/a/c/b0/d/i/d.java e/a/a/c/b0/d/i/a.java e/a/a/c/b0/e/c.java e/a/a/c/c/e.java e/a/a/c/c/a/b.java e/a/a/c/d/i.java e/a/a/c/d/a.java e/a/a/c/v/c.java e/a/a/c/b/i.java e/a/a/c/t0/e.java

ISSUE	SEVERITY	STANDARDS	FILES
			[illegible] e/a/a/b/e/n/a.java e/a/a/y/c.java e/c/a/u/b.java e/c/a/t/j.java e/c/a/v/b.java e/c/a/v/i.java e/c/a/v/j.java e/c/a/p/h.java e/c/a/p/g.java e/c/a/p/n/o.java e/c/a/p/n/e.java e/c/a/p/n/y.java e/c/a/p/n/m.java e/c/a/p/n/c0/i.java e/c/a/p/n/c0/m.java e/c/a/p/o/j.java e/c/a/p/o/g.java e/c/a/p/o/m.java e/c/a/p/p/g/f.java e/c/a/p/p/c/p.java e/c/a/p/p/c/s.java e/d/a/a/b.java e/d/a/a/a.java e/d/a/a/i/b/h.java e/d/a/a/i/b/d.java e/d/a/a/i/b/e.java e/d/a/a/i/b/j.java e/d/a/a/i/b/f.java e/d/a/a/i/b/g.java e/d/a/a/j/b.java e/d/a/a/j/e.java e/d/a/a/j/a.java e/d/a/a/j/r/i/b.java e/d/a/a/j/r/h/b.java e/d/a/a/j/r/h/c.java e/d/a/a/j/p/b.java e/d/a/a/j/p/c.java e/d/a/a/j/p/a.java e/d/a/c/j/h.java e/d/a/c/j/g.java e/d/a/b/g/a/s9.java e/d/a/b/g/a/p9.java e/d/a/b/f/e/l5.java e/d/a/b/f/e/o3.java e/d/a/b/f/e/j5.java e/d/a/b/f/e/o2.java e/d/a/b/f/e/c6.java e/d/a/b/f/e/b2.java e/d/a/b/f/e/z5.java e/d/a/b/f/e/b5.java e/d/a/b/f/e/l6.java e/d/a/b/c/p/d.java e/d/c/a/c0/e0.java e/d/c/a/t/a.java e/d/c/a/a0/e.java e/d/c/a/a0/f.java e/d/c/a/b0/c.java e/d/c/a/v/b.java e/d/c/a/y/b.java e/d/c/a/w/d.java e/d/c/a/w/e.java e/d/d/c.java e/d/d/n/a.java e/d/d/n/o/a.java e/d/d/n/p/b.java

ISSUE	SEVERITY	STANDARDS	FILES
			e/d/d/n/p/b.java e/d/d/n/p/a.java e/d/d/g/q.java e/d/d/g/p.java e/d/d/f/a/b.java e/d/d/q/a.java e/d/d/l/f0.java e/d/d/l/u0.java e/d/d/p/c.java e/d/e/o.java e/d/e/c.java e/d/e/k.java e/d/e/u.java e/d/e/l.java e/d/b/a/a.java e/d/b/c/d.java e/d/b/c/e.java e/d/b/c/g.java e/d/b/b/e.java e/e/a/i/a.java e/e/a/g/b0/o.java e/e/a/d/l/l.java e/e/a/b/a.java e/e/a/k/j.java l/a/b0.java l/a/j0.java l/a/p1.java l/a/a/v.java y/h.java y/i.java y/r/c.java y/t/c.java y/w/c/d.java y/w/c/g.java y/w/c/l.java
Insecure Implementation of SSL. Trusting all the certificates or accepting self signed certificates is a critical Security Hole. This application is vulnerable to MITM attacks	high	**CVSS V2:** 7.4 (high) **CWE:** CWE-295 - Improper Certificate Validation **OWASP Top 10:** M3: Insecure Communication **OWASP MASVS:** MSTG-NETWORK-3	z/j0/i/h/b.java
			b0/a/e/f.java v/u/d/d0.java v/u/d/r.java v/i/i/b.java v/i/g/b.java v/i/g/c.java v/i/g/d.java v/i/g/e.java v/i/g/f.java v/i/m/b.java v/i/m/n.java v/i/m/g.java v/i/m/r.java v/i/m/a.java v/i/e/b.java v/i/e/o.java v/i/e/c.java v/i/e/f.java v/i/l/a.java v/n/d/w.java v/n/d/o.java

ISSUE	SEVERITY	STANDARDS	FILES
			v/n/d/d.java v/n/d/q.java v/n/d/u.java v/n/d/x.java v/n/d/a.java v/g/b/b.java v/g/b/c.java v/t/j.java v/s/u/a.java v/a0/w.java v/a0/y.java v/a0/x.java v/b0/a/a/g.java v/e0/e.java v/e0/k.java v/m/a/a.java v/j/a/b.java v/v/i.java v/v/j.java v/v/k.java v/v/u.java v/b/q/a0.java v/b/q/w.java v/b/q/z0.java v/b/q/x0.java v/b/q/a1.java v/b/q/e0.java v/b/q/d1.java v/b/q/n0.java v/b/q/r0.java v/b/q/k0.java v/b/q/m0.java v/b/k/o.java v/b/k/h.java v/b/k/q.java v/b/k/e.java v/b/p/f.java v/b/p/i/d.java v/b/p/i/g.java v/k/b/a.java v/l/e.java v/y/a/c.java v/y/a/f/c.java v/p/a/a.java com/bumptech/glide/GeneratedAppGlideModuleImpl.java com/bumptech/glide/manager/SupportRequestManagerFragment.java com/imgzine/androidcore/CoreApplication.java com/imgzine/androidcore/CoreActivity.java com/imgzine/androidcore/content/ContentFragment.java com/imgzine/androidcore/content/settings/EditUserProfileFragment.java com/imgzine/androidcore/content/settings/SettingsFragment.java com/imgzine/androidcore/content/settings/BasicTableFragment.java com/imgzine/androidcore/content/settings/UserProfileFragment.java com/imgzine/androidcore/content/comments/CommentsFragment.java

ISSUE	SEVERITY	STANDARDS	FILES
The App logs information. Sensitive information should never be logged.	info	CVSS V2: 7.5 (high) CWE: CWE-532 - Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/imgzine/androidcore/content/reporter/EditPostFragment.java com/imgzine/androidcore/content/notification/NotificationCenterFragment.java com/imgzine/androidcore/content/plugin/PluginFragment.java com/imgzine/androidcore/content/mediaviewer/MediaViewerFragment.java com/imgzine/androidcore/content/peoplefinder/PeopleFinderFragment.java com/imgzine/androidcore/content/peoplefinder/profile/ProfileDetailFragment.java com/imgzine/androidcore/content/search/SearchFragment.java com/imgzine/androidcore/content/magazine/MagazineFragment.java com/imgzine/androidcore/content/messenger/MessengerFragment.java com/imgzine/androidcore/content/index/IndexFragment.java com/imgzine/androidcore/content/agenda/AgendaItemsListFragment.java com/imgzine/androidcore/content/article/ArticleDetailFragment.java com/imgzine/androidcore/content/custom/MasterDetailFragment.java com/imgzine/androidcore/engine/wizard/WizardFragment.java com/imgzine/androidcore/engine/workers/DownloadFileWorker.java com/imgzine/androidcore/engine/notifications/fcm/CoreFirebaseMessagingService.java com/imgzine/androidcore/grid/article/toolbar/ArticleToolBarView.java e/a/a/v.java e/a/a/f.java e/a/a/m.java e/a/a/d0/e.java e/a/a/z/f.java e/a/a/z/j/b/g.java e/a/a/a/b.java e/a/a/a/h.java e/a/a/a/e.java e/a/a/a/r/b/h.java e/a/a/a/a0/i.java e/a/a/a/a0/a.java e/a/a/a/b0/b.java e/a/a/a/p/b.java e/a/a/a/p/n.java e/a/a/a/p/o.java e/a/a/a/p/i.java e/a/a/a0/a.java e/a/a/b0/d2.java e/a/a/e0/b.java e/a/a/c/u0/b.java e/a/a/c/m0/b.java e/a/a/c/g0/d.java e/a/a/c/i0/i.java e/a/a/c/x0/i/f.java e/a/a/c/q0/b.java e/a/a/c/a/b.java e/a/a/c/a/h.java

ISSUE	SEVERITY	STANDARDS	FILES
			e/a/a/c/a/p.java e/a/a/c/a/j.java e/a/a/c/a/l.java e/a/a/c/a/a.java e/a/a/c/p0/b.java e/a/a/c/p0/d.java e/a/a/c/k0/c.java e/a/a/c/a0/o.java e/a/a/c/a0/a.java e/a/a/c/h0/a/d.java e/a/a/c/b0/d/a.java e/a/a/c/o0/c.java e/a/a/c/c/b.java e/a/a/c/c/n/b.java e/a/a/c/c/n/a.java e/a/a/c/c/g/h.java e/a/a/c/d/f.java e/a/a/c/v/a.java e/a/a/c/b/r.java e/a/a/c/t0/o/h.java e/a/a/c/t0/o/j.java e/a/a/c/t0/o/g.java e/a/a/c/t0/o/k.java e/a/a/b/a.java e/a/a/b/e/g.java e/a/a/b/e/k.java e/a/a/b/e/l.java e/a/a/y/b0.java e/c/a/c.java e/c/a/l.java e/c/a/t/j.java e/c/a/t/k/d.java e/c/a/t/k/j.java e/c/a/o/d.java e/c/a/o/e.java e/c/a/v/k/a.java e/c/a/q/e.java e/c/a/q/k.java e/c/a/q/l.java e/c/a/p/n/b0.java e/c/a/p/n/i.java e/c/a/p/n/j.java e/c/a/p/n/r.java e/c/a/p/n/l.java e/c/a/p/n/d0/e.java e/c/a/p/n/d0/j.java e/c/a/p/n/c0/i.java e/c/a/p/n/c0/j.java e/c/a/p/n/e0/a.java e/c/a/p/o/c.java e/c/a/p/o/d.java e/c/a/p/o/s.java e/c/a/p/o/f.java e/c/a/p/o/t.java e/c/a/p/m/b.java e/c/a/p/m/j.java e/c/a/p/m/l.java e/c/a/p/m/p/b.java e/c/a/p/p/a.java e/c/a/p/p/g/d.java e/c/a/p/p/g/j.java e/c/a/p/p/g/a.java e/c/a/p/p/c/a0.java e/c/a/p/p/c/c0.java

ISSUE	SEVERITY	STANDARDS	FILES
			e/c/a/p/p/c/n.java e/c/a/p/p/c/o.java e/c/a/p/p/c/c.java e/c/a/p/p/c/s.java e/c/a/p/p/c/l.java e/d/a/a/i/c.java e/d/a/a/i/e.java e/d/a/a/j/p/k.java e/d/a/c/o/a.java e/d/a/c/j/g.java e/d/a/b/i/a.java e/d/a/b/g/a/n4.java e/d/a/b/a/a/b.java e/d/a/b/a/a/a.java e/d/a/b/f/d/i.java e/d/a/b/f/e/b.java e/d/a/b/f/e/c1.java e/d/a/b/f/e/n8.java e/d/a/b/f/e/tc.java e/d/a/b/f/e/r5.java e/d/a/b/f/e/b1.java e/d/a/b/f/e/n1.java e/d/a/b/f/e/s1.java e/d/a/b/f/e/q1.java e/d/a/b/f/e/j1.java e/d/a/b/f/e/m1.java e/d/a/b/f/e/g2.java e/d/a/b/f/e/p1.java e/d/a/b/f/e/r1.java e/d/a/b/c/v.java e/d/a/b/c/b0.java e/d/a/b/c/e.java e/d/a/b/c/i.java e/d/a/b/c/j.java e/d/a/b/c/t.java e/d/a/b/c/o/c.java e/d/a/b/c/o/a.java e/d/a/b/c/m/b.java e/d/a/b/c/m/d.java e/d/a/b/c/m/e.java e/d/a/b/c/m/i.java e/d/a/b/c/m/h0.java e/d/a/b/c/m/y.java e/d/a/b/c/m/l.java e/d/a/b/c/m/a.java e/d/a/b/c/l/g/b.java e/d/a/b/c/l/g/p.java e/d/a/b/c/p/h.java e/d/a/b/c/p/d.java e/d/c/a/x/a/a.java e/d/d/c.java e/d/d/n/o/b.java e/d/d/n/p/c.java e/d/d/l/e1.java e/d/d/l/a0.java e/d/d/l/w.java e/d/d/l/n.java e/d/d/l/z.java e/d/d/l/g0.java e/d/d/l/e0.java e/d/d/l/c.java e/d/d/l/b0.java e/d/d/l/d.java e/d/d/l/p.java

ISSUE	SEVERITY	STANDARDS	FILES
			e/d/d/l/d0.java e/d/d/l/f0.java e/d/d/l/i.java e/d/d/l/h0.java e/d/d/l/g.java e/d/d/l/l0.java e/d/d/l/u0.java e/d/d/l/n0.java e/d/d/l/p0.java e/d/d/l/m.java e/d/d/l/i1.java e/d/d/l/t.java e/d/d/p/o.java e/d/d/p/q.java e/d/d/p/p.java e/d/d/p/e.java e/d/d/p/f.java e/d/d/p/g.java e/d/d/p/r.java e/d/d/p/a.java e/b/a/a/a.java
App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	high	**CVSS V2:** 5.9 (medium) **CWE:** CWE-89 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') **OWASP Top 10:** M7: Client Code Quality	v/v/i.java e/d/a/a/j/r/i/n.java e/d/a/a/j/r/i/o.java e/d/a/a/j/r/i/j.java e/d/a/b/g/a/j4.java e/d/a/b/g/a/s9.java e/d/a/b/g/a/d.java e/d/a/b/g/a/ja.java e/d/a/b/c/p/d.java
App creates temp file. Sensitive information should never be written into a temp file.	high	**CVSS V2:** 5.5 (medium) **CWE:** CWE-276 - Incorrect Default Permissions **OWASP Top 10:** M2: Insecure Data Storage **OWASP MASVS:** MSTG-STORAGE-2	v/v/u.java e/a/a/c/t0/o/k.java e/d/d/n/o/c.java
Files may contain hardcoded sensitive informations like usernames, passwords, keys etc.	high	**CVSS V2:** 7.4 (high) **CWE:** CWE-312 - Cleartext Storage of Sensitive Information **OWASP Top 10:** M9: Reverse Engineering **OWASP MASVS:** MSTG-STORAGE-14	e/a/a/c/w0/b.java e/c/a/p/n/q.java
MD5 is a weak hash known to have hash collisions.	high	**CVSS V2:** 7.4 (high) **CWE:** CWE-327 - Use of a Broken or Risky Cryptographic Algorithm **OWASP Top 10:** M5: Insufficient Cryptography **OWASP MASVS:** MSTG-CRYPTO-4	e/d/a/b/g/a/ba.java e/d/a/b/c/p/d.java
The App uses an insecure Random Number Generator.	high	**CVSS V2:** 7.5 (high) **CWE:** CWE-330 - Use of Insufficiently Random Values **OWASP Top 10:** M5: Insufficient Cryptography **OWASP MASVS:** MSTG-CRYPTO-6	e/d/a/b/g/a/ba.java e/d/d/f/b.java l/a/q2/a.java
This App may have root detection capabilities.	secure	**CVSS V2:** 0 (info) **OWASP MASVS:** MSTG-RESILIENCE-1	e/d/a/b/f/e/q1.java
The App uses ECB mode in Cryptographic encryption algorithm. ECB mode is known to be weak as it results in the same ciphertext for identical blocks of plaintext.	high	**CVSS V2:** 5.9 (medium) **CWE:** CWE-327 - Use of a Broken or Risky Cryptographic Algorithm **OWASP Top 10:** M5: Insufficient Cryptography **OWASP MASVS:** MSTG-CRYPTO-2	e/d/c/a/c0/d.java

ISSUE	SEVERITY	STANDARDS	FILES
SHA-1 is a weak hash known to have hash collisions.	high	**CVSS V2:** 5.9 (medium) **CWE:** CWE-327 - Use of a Broken or Risky Cryptographic Algorithm **OWASP Top 10:** M5: Insufficient Cryptography **OWASP MASVS:** MSTG-CRYPTO-4	e/d/d/l/e1.java

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
www.slf4j.org	good	**IP:** 83.173.251.158 **Country:** Switzerland **Region:** Zurich **City:** Zurich **Latitude:** 47.366669 **Longitude:** 8.55 **View:** Google Map
plus.google.com	good	**IP:** 172.217.167.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
app-measurement.com	good	**IP:** 172.217.167.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
schemas.android.com	good	No Geolocation information available.
www.google.com	good	**IP:** 172.217.25.132 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.googleadservices.com	good	**IP:** 216.58.200.98 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
infectieradar-rivm.firebaseio.com	good	**IP:** 35.201.97.85 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
pagead2.googlesyndication.com	good	**IP:** 216.58.199.66 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
goo.gl	good	**IP:** 216.58.203.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
ns.adobe.com	good	No Geolocation information available.
platform.nlinzorg.nl	good	**IP:** 51.145.255.223 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.88969 **View:** Google Map
firebase.google.com	good	**IP:** 216.58.196.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
google.com	good	**IP:** 216.58.200.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
proxy.nlinzorg.nl	good	**IP:** 51.145.255.223 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.88969 **View:** Google Map

URLS

URL	FILE
http://www.slf4j.org/codes.html#StaticLoggerBinder http://www.slf4j.org/codes.html#multiple_bindings http://www.slf4j.org/codes.html#unsuccessfulInit http://www.slf4j.org/codes.html#replay http://www.slf4j.org/codes.html#substituteLogger http://www.slf4j.org/codes.html#version_mismatch http://www.slf4j.org/codes.html#loggerNameMismatch	b0/a/c.java
http://ns.adobe.com/xap/1.0/	v/m/a/a.java
http://schemas.android.com/apk/res/android	v/b/k/o.java
https://platform.nlinzorg.nl/	com/imgzine/androidcore/CoreApplication.java
https://proxy.nlinzorg.nl/	com/imgzine/androidcore/engine/workers/DownloadFileWorker.java
https://platform.nlinzorg.nl/	e/a/a/a/c/a.java
https://platform.nlinzorg.nl/	e/a/a/c/n0/a.java
https://proxy.nlinzorg.nl/	e/a/a/c/g0/f.java
https://platform.nlinzorg.nl/	e/a/a/c/g0/h/a.java
https://platform.nlinzorg.nl/	e/a/a/c/y/c.java
data:image	e/c/a/p/o/e.java
www.google.com https://www.google.com https://goo.gl/NAOOOI. https://goo.gl/NAOOOI	e/d/a/b/g/a/ba.java
https://app-measurement.com/a	e/d/a/b/g/a/o.java
https://google.com/search?	e/d/a/b/g/a/o7.java

URL	FILE
https://www.googleadservices.com/pagead/conversion/app/deeplink?id_type=adid&sdk_version=%s&rdid=%s&bundleid=%s&retry=%s	e/d/a/b/g/a/v6.java
https://firebase.google.com/support/guides/disable-analytics	e/d/a/b/g/a/g4.java
https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps	e/d/a/b/a/a/b.java
https://goo.gl/J1sWQy	e/d/a/b/f/e/tc.java
https://app-measurement.com/a	e/d/a/b/f/e/s7.java
https://plus.google.com/	e/d/a/b/c/m/a0.java
https://%s/%s/%s?key=%s	e/d/d/n/e.java
https://infectieradar-rivm.firebaseio.com	Android String Resource

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://infectieradar-rivm.firebaseio.com	info App talks to a Firebase Database.

EMAILS

EMAIL	FILE
this@apply.icon	e/a/a/y/i.java
u0013android@android.com0 u0013android@android.com	e/d/a/b/c/a0.java

TRACKERS

TRACKER	URL
Google Firebase Analytics	https://reports.exodus-privacy.eu.org/trackers/49

PLAYSTORE INFORMATION

Title: COVID Radar

Score: 3.18 **Installs:** 50,000+ **Price:** 0 **Android Version Support:** 6.0 and up **Category:** Medical **Play Store URL:** nl.lumc.covidradar

Developer Details: LUMC Leiden, LUMC+Leiden, None, https://www.lumc.nl, covidradar@lumc.nl,

Release Date: Mar 27, 2020 **Privacy Policy:** Privacy link

Description:

Met deze app verzamelen we gegevens van Nederlanders voor wetenschappelijk onderzoek naar het bestrijden van het coronavirus (COVID-19). We willen beter kunnen gaan voorspellen welke zorgbehoefte er in Nederland straks is: hoeveel corona-patiënten verwachten we waar en wanneer? Dit is een app van het Leids Universitair Medisch Centrum (LUMC). Alle gegevens worden anoniem verwerkt. De geanonimiseerde gegevens worden veilig opgeslagen in Nederland. Lees hierover meer in de disclaimer. In Nederland testen we beperkt of mensen het coronavirus hebben. We testen iemand alleen als hij/zij symptomen heeft en tot een kwetsbare doelgroep behoort. Hierdoor weten we niet precies hoeveel mensen in Nederland besmet zijn met het virus. Door van zoveel mogelijk mensen in Nederland gegevens te verzamelen, kunnen we onderzoeken hoeveel mensen het coronavirus hebben (gehad) en waar zij in Nederland verblijven. Met deze gegevens proberen we de toekomstige zorgvraag te voorspellen: hoeveel coronapatiënten verwachten we waar en wanneer? Uw bijdrage aan dit onderzoek is erg belangrijk om de behoefte aan zorg te kunnen voorspellen. Help mee! Samen tegen het coronavirus in Nederland! Deze app is een initiatief van het Leids Universitair Medisch Centrum (LUMC), gesteund door het Landelijk Netwerk Acute Zorg (LNAZ). Installeer de app en deel regelmatig gegevens over uw fysieke gesteldheid en die van uw huisgenoten voor wetenschappelijk onderzoek. Stimuleer familie, vrienden, kennissen en collega’s om hetzelfde te doen. Samen tegen het coronavirus in Nederland!

App Security Score Calculation

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

Risk Calculation

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

Report Generated by - MobSF v3.0.8 Beta

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.