ANDROID STATIC ANALYSIS REPORT

Aarogya Setu (1.5.2)

File Name:	Aarogya Setu_v1.5.2_apkpure.com.xapk
Package Name:	nic.goi.aarogyasetu
Average CVSS Score:	0
App Security Score:	100/100 (LOW RISK)
Trackers Detection:	2/421
Scan Date:	Feb. 20, 2022, 7:31 p.m.

FILE INFORMATION

File Name: Aarogya Setu_v1.5.2_apkpure.com.xapk
Size: 3.29MB
MD5: 501efa5c58f3dbc95cd320cac7f9b603

SHA1: af5aa45e3accf4dd57d0d0875d544b418815c18b

SHA256: c4bad9d0ab8044a512d0321a86f061c65d369f1fc25b6bbfa38e213ea4c3e067

APP INFORMATION

App Name: Aarogya Setu

Package Name: nic.goi.aarogyasetu

Main Activity: nic.goi.aarogyasetu.views.SplashActivity

Target SDK: 30

Min SDK: 21

Max SDK:

Android Version Name: 1.5.2

Android Version Code: 1060

APP COMPONENTS

Activities: 15

Services: 13

Receivers: 13

Providers: 3

Exported Activities: 0

Exported Services: 2

Exported Receivers: 4

Exported Providers: 0

CERTIFICATE INFORMATION

```
APK is signed
v1 signature: True
v2 signature: True
v3 signature: True
Found 1 unique certificates
Subject: C=91, ST=Delhi, L=New Delhi, O=NITI Aayog, OU=NITI Aayog, CN=NITI Aayog
```

Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-03-28 06:18:35+00:00
Valid To: 2045-03-22 06:18:35+00:00
Issuer: C=91, ST=Delhi, L=New Delhi, O=NITI Aayog, OU=NITI Aayog, CN=NITI Aayog
Serial Number: 0xba294b3
Hash Algorithm: sha256
md5: 34073824749a0a089c167ef8abc9cc4b
sha1: 2c848c2d2bc92cfb2aa7f5eac3bd391922555251
sha256: c70f65be3100a5f7d5fa05b7c170bda1d7345b5a3868d5af6dc3f4146000ad88
sha512: b905e59a3f0e7549f457bddb9ada134ce8ea8b2b5c331b2bf0d26f33e1a9ce2c3dc4c20a6e3175c34cf92349c7badbdc4b8f17b92c1516041649681b999d4e74
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 91919c7af17c205d1a3c9c91f51877d2cd74d34df33b9ea86e8b6b4fee4d53d5

STATUS	DESCRIPTION
secure	Application is signed with a code signing certificate
warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.ACCESS_NETWORK_STPermisATE	unknown	Unknown permission	Unknown permission from android reference
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.ACCESS_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
com.google.android.c2dm.permission.RECEIVE	signature	C2DM permissions	Permission for cloud to device messaging.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.TAGS check
possible VM check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
nic.goi.aarogyasetu.views.SplashActivity	Schemes: https://, Hosts: www.aarogyasetu.gov.in, Path Prefixes: /app,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	good	Base config is configured to disallow clear text traffic to all domains.

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.
2	Broadcast Receiver (nic.goi.aarogyasetu.background.BootReceiver) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
3	Broadcast Receiver (nic.goi.aarogyasetu.utility.SmsReceiver) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
4	Broadcast Receiver (nic.goi.aarogyasetu.utility.BluetoothLocationReceiver) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.

NO	ISSUE	SEVERITY	DESCRIPTION
5	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.
6	Service (com.google.android.play.core.assetpacks.AssetPackExtractionService) is not Protected. [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.
7	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.

CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
google.com	good	**IP:** 172.217.14.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.google.com	good	**IP:** 142.251.33.68 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
static.swaraksha.gov.in	good	**IP:** 3.109.44.91 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
e.crashlytics.com	good	No Geolocation information available.
web.swaraksha.gov.in	good	**IP:** 13.235.25.222 **Country:** India **Region:** Maharashtra **City:** Mumbai **Latitude:** 19.014410 **Longitude:** 72.847939 **View:** Google Map
pagead2.googlesyndication.com	good	**IP:** 142.250.217.66 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
journeyapps.com	good	**IP:** 65.8.68.104 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
app-measurement.com	good	**IP:** 142.251.33.110 **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.
tools.ietf.org	good	**IP:** 4.31.198.62 **Country:** United States of America **Region:** California **City:** San Jose **Latitude:** 37.339390 **Longitude:** -121.894958 **View:** Google Map
settings.crashlytics.com	good	No Geolocation information available.
plus.google.com	good	**IP:** 172.217.14.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.googleadservices.com	good	**IP:** 142.250.69.194 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
apps.apple.com	good	**IP:** 23.73.34.217 **Country:** Canada **Region:** Alberta **City:** Calgary **Latitude:** 51.050110 **Longitude:** -114.085289 **View:** Google Map
goo.gl	good	**IP:** 142.250.217.78 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
covid19-6c396.firebaseio.com	good	**IP:** 35.201.97.85 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api.swaraksha.gov.in	good	**IP:** 13.126.220.240 **Country:** India **Region:** Maharashtra **City:** Mumbai **Latitude:** 19.014410 **Longitude:** 72.847939 **View:** Google Map
github.com	good	**IP:** 140.82.112.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
fp.swaraksha.gov.in	good	**IP:** 52.66.115.223 **Country:** India **Region:** Maharashtra **City:** Mumbai **Latitude:** 19.014410 **Longitude:** 72.847939 **View:** Google Map
firebase.google.com	good	**IP:** 142.250.217.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
play.google.com	good	**IP:** 142.250.69.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

URLS

URL	FILE
https://web.swaraksha.gov.in/ncv19	e/a/a/a/i.java
https://play.google.com/store/apps/details?id=nic.goi.aarogyasetu https://apps.apple.com/in/app/aarogyasetu/id1505825357	e/a/a/a/n.java
https://api.swaraksha.gov.in/	e/a/a/a/z.java
https://fp.swaraksha.gov.in/	e/a/a/m/c.java
https://api.swaraksha.gov.in/	e/a/a/q/k.java
https://tools.ietf.org/html/rfc7518#section-3.2 https://tools.ietf.org/html/rfc7518#section-3.4 https://tools.ietf.org/html/rfc7518#section- https://tools.ietf.org/html/rfc7518#section-3.3	io/jsonwebtoken/SignatureAlgorithm.java

URL	FILE
https://github.com/jwtk/jjwt#custom-json-processor https://github.com/jwtk/jjwt#json-jackson-custom-types	io/jsonwebtoken/impl/DefaultClaims.java
https://tools.ietf.org/html/rfc7518#section-3.2	io/jsonwebtoken/security/Keys.java
https://web.swaraksha.gov.in/ncv19	nic/goi/aarogyasetu/firebase/FcmMessagingService.java
javascript:window. https://web.swaraksha.gov.in/ncv19?locale= https://play.google.com/store/apps/details?id=nic.goi.aarogyasetu https://apps.apple.com/in/app/aarogyasetu/id1505825357 https://web.swaraksha.gov.in/ncv19/privacy/ https://static.swaraksha.gov.in/tnc/ https://web.swaraksha.gov.in/ncv19	nic/goi/aarogyasetu/views/HomeActivity.java
https://play.google.com/store/apps/details?id=nic.goi.aarogyasetu https://apps.apple.com/in/app/aarogyasetu/id1505825357 https://web.swaraksha.gov.in/ncv19	nic/goi/aarogyasetu/views/PermissionActivity.java
https://web.swaraksha.gov.in/ncv19	nic/goi/aarogyasetu/views/SplashActivity.java
https://web.swaraksha.gov.in/ncv19/account-delete/	nic/goi/aarogyasetu/views/settings/DeleteAccountActivity.java
http://schemas.android.com/apk/res/android	p/a/a/b/a.java
data:image	r/b/a/m/u/e.java
https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps	r/c/a/b/a/a/a.java
https://plus.google.com/	r/c/a/b/d/l/k0.java

URL	FILE
https://goo.gl/J1sWQy	r/c/a/b/g/g/h.java
https://app-measurement.com/a	r/c/a/b/g/g/z7.java
https://google.com/search?	r/c/a/b/i/b/e7.java
https://www.googleadservices.com/pagead/conversion/app/deeplink?id_type=adid&sdk_version=%s&rdid=%s&bundleid=%s&retry=%s	r/c/a/b/i/b/f6.java
https://app-measurement.com/a	r/c/a/b/i/b/p.java
www.google.com https://www.google.com https://goo.gl/NAOOOI. https://goo.gl/NAOOOI	r/c/a/b/i/b/s9.java
https://firebase.google.com/support/guides/disable-analytics	r/c/a/b/i/b/t3.java
https://%s/%s/%s https://firebase.google.com/support/privacy/init-options.	r/c/d/m/g.java
https://e.crashlytics.com/spi/v2/events	u/a/a/a/o/g/j.java
https://settings.crashlytics.com/spi/v2/platforms/android/apps/%s/settings	u/a/a/a/o/g/p.java
https://covid19-6c396.firebaseio.com https://journeyapps.com/ https://github.com/journeyapps/zxing-android-embedded https://static.swaraksha.gov.in/tnc/ https://web.swaraksha.gov.in/ncv19/privacy/	Android String Resource

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://covid19-6c396.firebaseio.com	info App talks to a Firebase Database.

EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	r/c/a/b/d/a0.java

TRACKERS

TRACKER	CATEGORIES	URL
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

HARDCODED SECRETS

POSSIBLE SECRETS
"firebase_database_url" : "https://covid19-6c396.firebaseio.com"
"google_api_key" : "AIzaSyCgqPpLQ5fRS9imi6g3CmFYbluHxqp9HkE"
"google_crash_reporting_api_key" : "AIzaSyCgqPpLQ5fRS9imi6g3CmFYbluHxqp9HkE"
"library_zxingandroidembedded_author" : "JourneyApps"
"library_zxingandroidembedded_authorWebsite" : "https://journeyapps.com/"

PLAYSTORE INFORMATION

Title: Aarogya Setu

Score: 3.3794117 **Installs:** 100,000,000+ **Price:** 0 **Android Version Support:** 5.0 and up **Category:** Health & Fitness **Play Store URL:** nic.goi.aarogyasetu

Developer Details: National Informatics Centre., 9076108670215860604, National Informatics Centre, Ministry of Electronics & IT (MeitY) A-Block, Lodhi Road, CGO Complex New Delhi-110003, None, support.aarogyasetu@gov.in,

Release Date: Apr 11, 2020 **Privacy Policy:** Privacy link

Description:

Aarogya Setu is a mobile application developed by the Government of India to connect essential health services with the people of India in our combined fight against COVID-19. The App is aimed at augmenting the initiatives of the Government of India, particularly the Department of Health, in proactively reaching out to and informing the users of the app regarding risks, best practices and relevant advisories pertaining to the containment of COVID-19. The following are some of the key features of the Aarogyasetu platform : • Automatic contact tracing using Bluetooth • Self-Assessment test based on ICMR guidelines • Facilitates the Registration for Covid-19 vaccine registration • Facilitates the download of Covid-19 vaccine certificate • Open API based Health Status Check • Hotspot Forecasting • Updates, advisory and best practices related to COVID-19 • Integration with e-Pass • Geo-location based COVID-19 statistics • Nation-wide COVID-19 statistics • Emergency COVID-19 Helpline contacts • List of ICMR approved Labs with COVID-19 testing facilities • Provides the infection/Risk Status of User • QR Code scan feature to share Risk Status • Recent Contacts Feature to check health status of recent contacts • Support for over 12 Languages Key Permissions required by the App : • Bluetooth and Background Location permission for Contact tracing • Camera permission for scanning QR code

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 v3.4.5 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.