ANDROID STATIC ANALYSIS REPORT

Immuni (2.6.0)

File Name:	it.ministerodellasalute.immuni_2.6.0-2641892_minAPI24(arm64-v8a,armeabi-v7a,x86,x86_64)(nodpi)_apkmirror.com.apk
Package Name:	it.ministerodellasalute.immuni
Average CVSS Score:	0
App Security Score:	100/100 (LOW RISK)
Scan Date:	June 3, 2022, 1:46 a.m.

FILE INFORMATION

File Name: it.ministerodellasalute.immuni_2.6.0-2641892_minAPI24(arm64-v8a,armeabi-v7a,x86,x86_64)(nodpi)_apkmirror.com.apk
Size: 32.43MB
MD5: d0d855b87e49faded81fc018949afd1b
SHA1: 2f97cbe77447c7771fd4b3532652dc6c39f86af4
SHA256: c1bdd2f9d35bd7cd1b605457e17afa803fcb9552142790841184db2d55be694e

APP INFORMATION

App Name: Immuni
Package Name: it.ministerodellasalute.immuni
Main Activity: it.ministerodellasalute.immuni.ui.setup.SetupActivity
Target SDK: 30
Min SDK: 24
Max SDK:
Android Version Name: 2.6.0
Android Version Code: 2641892

APP COMPONENTS

Activities: 13
Services: 5
Receivers: 9
Providers: 2
Exported Activities: 0
Exported Services: 2
Exported Receivers: 2
Exported Providers: 0

CERTIFICATE INFORMATION

APK is signed
v1 signature: False
v2 signature: True
v3 signature: True
Found 1 unique certificates
Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-05-18 14:31:05+00:00
Valid To: 2050-05-18 14:31:05+00:00

Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xfcf83c2889029113d147c82d917b30228e8d4f3
Hash Algorithm: sha256
md5: 72cf2a66720919c8724eb0172d0fdebe
sha1: b325bf04d0f8d056b4dd45b09bb87cc4e5ce5d76
sha256: f7d3efcb083f2829c1a3d8a03b5e487e029499c9f6966e1ed6c64c1e233607f9
sha512: 2d19c4c208c38682b9a546f2025b570a8ecabc4e44eb2b51476c15c81797f47aa614c8e0869f0a5fa1f65465807214101f047fb4e02067f1427646fecd6dbe00
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: cf5872457daf26fe5cb479b852ad385afb8b9fdda9780b06ae05af4a0ac417cb

STATUS	DESCRIPTION
secure	Application is signed with a code signing certificate

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.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</td></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
<tr><td>classes2.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.BOARD check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes3.dex</td><td><table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr></table></td></tr>
<tr><td>classes4.dex</td><td><table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Compiler</td><td>r8</td></tr></table></td></tr>
</table>

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	Broadcast Receiver (it.ministerodellasalute.immuni.receivers.UpdateReceiver) 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
2	Broadcast Receiver (it.ministerodellasalute.immuni.receivers.ExposureNotificationReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.nearby.exposurenotification.EXPOSURE_CALLBACK [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.
3	Service (com.google.android.gms.nearby.exposurenotification.WakeUpService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.nearby.exposurenotification.EXPOSURE_CALLBACK [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.
4	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

NO	ISSUE	SEVERITY	STANDARDS	FILES

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	lib/arm64-v8a/libconscrypt_jni.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	True info The shared object has the following fortified functions: ['__memmove_chk', '__strchr_chk', '__memset_chk', '__memcpy_chk', '__vsnprintf_chk', '__read_chk', '__strlen_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	lib/armeabi-v7a/libconscrypt_jni.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	lib/x86/libconscrypt_jni.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	lib/x86_64/libconscrypt_jni.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	True info The shared object has the following fortified functions: ['__strlen_chk', '__vsnprintf_chk', '__strchr_chk', '__memcpy_chk', '__memset_chk', '__read_chk', '__memmove_chk']	True info Symbols are stripped.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
github.com	good	**IP:** 140.82.114.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
journeyapps.com	good	**IP:** 65.8.66.23 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
ec.europa.eu	good	**IP:** 147.67.210.30 **Country:** Luxembourg **Region:** Luxembourg **City:** Luxembourg **Latitude:** 49.611671 **Longitude:** 6.130000 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
get.immuni.gov.it	good	**IP:** 23.200.86.74 **Country:** France **Region:** Ile-de-France **City:** Paris **Latitude:** 48.853409 **Longitude:** 2.348800 **View:** Google Map
www.w3.org	good	**IP:** 128.30.52.100 **Country:** United States of America **Region:** Massachusetts **City:** Cambridge **Latitude:** 42.365078 **Longitude:** -71.104523 **View:** Google Map
javax.xml.xmlconstants	good	No Geolocation information available.
www.salute.gov.it	good	**IP:** 104.18.21.233 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
analytics.immuni.gov.it	good	**IP:** 217.175.50.250 **Country:** Italy **Region:** Lazio **City:** Rome **Latitude:** 41.894741 **Longitude:** 12.483900 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.immuni.italia.it	good	**IP:** 2.16.165.204 **Country:** France **Region:** Ile-de-France **City:** Paris **Latitude:** 48.853409 **Longitude:** 2.348800 **View:** Google Map
id.uvci.eu	good	No Geolocation information available.
reopen.europa.eu	good	**IP:** 139.191.221.32 **Country:** Italy **Region:** Lombardia **City:** Milan **Latitude:** 45.464272 **Longitude:** 9.189510 **View:** Google Map
upload.immuni.gov.it	good	**IP:** 217.175.50.249 **Country:** Italy **Region:** Lazio **City:** Rome **Latitude:** 41.894741 **Longitude:** 12.483900 **View:** Google Map
my.site	good	**IP:** 3.64.163.50 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
apache.org	good	**IP:** 151.101.2.132 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
127.0.0.1	good	**IP:** 127.0.0.1 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
semver.org	good	**IP:** 185.199.110.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
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

DOMAIN	STATUS	GEOLOCATION
www.openuri.org	good	**IP:** 64.190.63.111 **Country:** Germany **Region:** Nordrhein-Westfalen **City:** Koeln **Latitude:** 50.933331 **Longitude:** 6.950000 **View:** Google Map
json-schema.org	good	**IP:** 104.21.8.16 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

🌐 URLS

URL	FILE
file:///android_asset/	com/bumptech/glide/load/model/AssetUriLoader.java
data:image	com/bumptech/glide/load/model/DataUrlLoader.java
http://javax.xml.XMLConstants/feature/secure-processing http://apache.org/xml/features/disallow-doctype-decl http://apache.org/xml/features/nonvalidating/load-external-dtd	com/fasterxml/jackson/databind/ext/DOMDeserializer.java

URL	FILE
http://json-schema.org/draft-04/schema# http://json-schema.org/draft-03/schema# http://json-schema.org/draft-04/hyper-schema#	com/github/fge/jsonschema/SchemaVersion.java
http://my.site/schemas/fstab.json#	com/github/fge/jsonschema/examples/Example6.java
http://my.site/myschema#	com/github/fge/jsonschema/examples/Example8.java
http://my.site/myschema#	com/github/fge/jsonschema/examples/Example9.java
https://json-schema.org/draft/2020-12/schema https://id.uvci.eu/DGC.combined-schema.json https://semver.org/ https://ec.europa.eu/health/sites/health/files/ehealth/docs/vaccination-proof_interoperability-guidelines_en.pdf	dgca/verifier/app/decoder/JsonSchemaKt.java
https://get.immuni.gov.it/docs/faq-	it/ministerodellasalute/immuni/api/services/ConfigurationSettingsServiceKt$defaultSettings$1.java
https://www.immuni.italia.it/app-tou.html	it/ministerodellasalute/immuni/api/services/ConfigurationSettingsServiceKt$defaultSettings$2.java
https://www.immuni.italia.it/app-pn.html	it/ministerodellasalute/immuni/api/services/ConfigurationSettingsServiceKt$defaultSettings$3.java
https://play.google.com/store/apps/details?id=	it/ministerodellasalute/immuni/extensions/playstore/PlayStoreActions.java
https://play.google.com/store/apps/details?id=	it/ministerodellasalute/immuni/logic/notifications/AppNotificationManager.java
http://127.0.0.1	org/mozilla/javascript/tools/debugger/Dim.java

URL	FILE
http://www.openuri.org/fragment	org/mozilla/javascript/xml/impl/xmlbeans/XML.java
http://www.w3.org/2000/xmlns/	org/mozilla/javascript/xmlimpl/XmlNode.java
http://localhost/	retrofit2/Response.java
https://analytics.immuni.gov.it https://upload.immuni.gov.it https://get.immuni.gov.it https://reopen.europa.eu https://journeyapps.com/ https://github.com/journeyapps/zxing-android-embedded https://www.immuni.italia.it/ https://www.salute.gov.it/portale/nuovocoronavirus/dettaglioFaqNuovoCoronavirus.jsp?lingua=italiano&id=244#19	Android String Resource

✉ EMAILS

EMAIL	FILE
appro@openssl.org	lib/arm64-v8a/libconscrypt_jni.so

HARDCODED SECRETS

POSSIBLE SECRETS
"const_authcode" : "AUTHCODE-"
"green_pass_select_type_token" : "Select type"
"library_zxingandroidembedded_author" : "JourneyApps"
"library_zxingandroidembedded_authorWebsite" : "https://journeyapps.com/"
"onboarding_exposure_api_not_activated" : "Exposure notifications not enabled"
"upload_data_missing_authorization_close" : "Close"
"upload_data_missing_authorization_enable" : "Enable"
"upload_data_missing_authorization_title" : "Reactivate exposure notifications to continue"
"green_pass_select_type_token" : "Art auswählen"
"onboarding_exposure_api_not_activated" : "Expositionsmeldungen nicht aktiviert"
"upload_data_missing_authorization_close" : "Schließen"
"upload_data_missing_authorization_enable" : "Aktivieren"
"upload_data_missing_authorization_title" : "Aktivieren Sie die Expositionsmeldungen"
"green_pass_select_type_token" : "Sélectionner le genre"
"onboarding_exposure_api_not_activated" : "Notifications de risque d'exposition désactivées"

POSSIBLE SECRETS
"upload_data_missing_authorization_close" : "Fermer"
"upload_data_missing_authorization_enable" : "Activer"
"upload_data_missing_authorization_title" : "Réactivez les notifications d'exposition pour continuer"
"green_pass_select_type_token" : "Selecciona tipo"
"onboarding_exposure_api_not_activated" : "Notificaciones de exposición sin activar"
"upload_data_missing_authorization_close" : "Cerrar"
"upload_data_missing_authorization_enable" : "Activar"
"upload_data_missing_authorization_title" : "Reactiva las notificaciones de exposición para continuar"
"green_pass_select_type_token" : "Seleziona tipologia"
"onboarding_exposure_api_not_activated" : "Notifiche di esposizione non attivate"
"upload_data_missing_authorization_close" : "Chiudi"
"upload_data_missing_authorization_enable" : "Attiva"
"upload_data_missing_authorization_title" : "Riattiva le notifiche di esposizione per continuare"

PLAYSTORE INFORMATION

Title: Immuni

Score: 3.31 **Installs:** 10,000,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** it.ministerodellasalute.immuni

Developer Details: Ministero della Salute, Ministero+della+Salute, None, https://www.immuni.italia.it/, cittadini@immuni.italia.it,

Release Date: Jun 1, 2020 **Privacy Policy:** Privacy link

Description:

Immuni is the official exposure notification app of the Italian government, developed by the Extraordinary Commissioner for the COVID-19 Emergency, in collaboration with the Ministry of Health and the Ministry for Innovation Technology and Digitalization. The app is developed and released in full compliance with the protection of the user's personal data and with current legislation, including the law-decree of April 30, 2020, n. 28. In the fight against the COVID-19 epidemic, the app aims to notify users at risk of carrying the virus as early as possible—even when they are asymptomatic. These users can then self-isolate to avoid infecting others, minimising the spread of the virus and speeding up the return to normal life for the majority of the population. By being alerted early, these users can also contact their general practitioner promptly and lower the risk of serious consequences. Since June 2021 the App is one of the access points to get the EU Digital COVID Certificate, a digital document implemented at EU level to facilitate safe free movement of the European citizens during the pandemic. The Certificate is a digital proof that a person has either been vaccinated against COVID-19, received a negative test result or recovered from COVID-19. The EU Digital COVID Certificate, released by the Ministry of Health, in compliance with EU standards contains a QR code with a digital signature to protect it against falsification. Through a specific Verifier App the QR code can be validated and authenticated. The system is based on Bluetooth Low Energy technology, which is designed to be especially energy-efficient, and it doesn’t collect any geolocation data, including GPS data. The app does not (and cannot) collect any data that would identify the user, such as their name, date of birth, address, telephone number, or email address. Therefore, Immuni is able to determine that contact has taken place between two users without knowing who those users are and where the contact occurred. Here is a list of some of the measures by which Immuni protects the user’s privacy: • The minimum amount of data is collected—only data which is strictly necessary to support and improve the exposure notification system. • The Bluetooth Low Energy code transmitted by the app is generated randomly and does not contain any information about the user's smartphone, let alone the user. In addition, this code changes several times every hour, protecting user privacy even more. • The data saved on the smartphone is encrypted. • The connections between the app and the server are encrypted. • All data, whether stored on the device or on the server, is deleted when no longer relevant, and certainly no later than December 31, 2021. • The Ministry of Health is the body that collects the data and decides for which purposes to use it. The data is used solely with the aim of containing the COVID-19 epidemic or for scientific research. • The data is stored on servers in Italy and managed by public bodies. Immuni does not and cannot diagnose. Based on the user’s history of exposure to potentially contagious users, it makes recommendations about what to do next. However, the app is not a medical device and is certainly not a substitute for a doctor. Immuni is a valuable tool in the fight against this horrendous epidemic, and every single user increases its overall effectiveness. It is strongly recommended to install the app, use it correctly, and encourage friends and loved ones to do likewise. However, nobody is compelled to use it. It is entirely the individual’s choice.

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.