

IOS STATIC ANALYSIS REPORT



GreenPass (1.4.2)

File Name:	GreenPass.ipa
Identifier:	com.italinnovation.greenPass
Scan Date:	May 7, 2022, 12:48 p.m.
App Security Score:	25/100 (CRITICAL RISK)
Grade:	F
Trackers Detection:	2/428

FINDINGS SEVERITY

兼 HIGH	▲ WARNING	i INFO	✓ SECURE
3	3	1	0

FILE INFORMATION

File Name: GreenPass.ipa

Size: 65.76MB

MD5: 1621c759d884747be2b37d282d4d306d

SHA1: 48e58a3961353f5b9541572d9a39bcff45f4dce7

SHA256: dbaac2c34ceba0c0b29122cfb69d0e80796eca81e8358af869d3bb1359113621

i APP INFORMATION

App Name: GreenPass

App Type: Swift

Identifier: com.italinnovation.greenPass

SDK Name: iphoneos15.4

Version: 1.4.2 Build: 1

Platform Version: 15.4

Min OS Version: 13.0

Supported Platforms: iPhoneOS,

Ad BINARY INFORMATION

Arch: ARM64

Sub Arch: CPU_SUBTYPE_ARM64_ALL

Bit: 64-bit Endian: <

᠄≡ APPLICATION PERMISSIONS

PERMISSIONS	STATUS	DESCRIPTION	REASON IN MANIFEST
NSCameraUsageDescription	dangerous	Access the Camera.	L'app ha bisogno di accedere alla camera per scannerizzare i QR Code
NSPhotoLibraryUsageDescription	dangerous	Access the user's photo library.	L'app ha bisogno di accedere alla galleria per caricare le immagini con il QR Code

</> IPA BINARY CODE ANALYSIS

NO	ISSUE SEVERITY	STANDARDS	DESCRIPTION
----	----------------	-----------	-------------

NO	ISSUE	SEVERITY	STANDARDS	DESCRIPTION
1	Binary makes use of insecure API(s)	high	CWE: CWE-676: Use of Potentially Dangerous Function OWASP Top 10: M7: Client Code Quality OWASP MASVS: MSTG- CODE-8	The binary may contain the following insecure API(s) _chmod , _wcslen , _printf , _strncat , _sscanf , _strtok , _sprintf , _strcpy , _strncpy , _vsnprintf , _stat , _strcat , _memcpy , _fopen , _strlen
2	Binary makes use of the insecure Random function(s)	high	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	The binary may use the following insecure Random function(s) _random , _srand
3	Binary makes use of Logging function	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG- STORAGE-3	The binary may use _NSLog function for logging.
4	Binary makes use of malloc function	high	CWE: CWE-789: Uncontrolled Memory Allocation OWASP Top 10: M7: Client Code Quality OWASP MASVS: MSTG- CODE-8	The binary may use _malloc function instead of calloc



PROTECTION	STATUS	SEVERITY	DESCRIPTION
NX	True	info	The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.
PIE	True	info	The binary is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.
STACK CANARY	True	info	This binary 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.
ARC	True	info	The binary is compiled with Automatic Reference Counting (ARC) flag. ARC is a compiler feature that provides automatic memory management of Objective-C objects and is an exploit mitigation mechanism against memory corruption vulnerabilities.
RPATH	True	warning	The binary has Runpath Search Path (@rpath) set. In certain cases an attacker can abuse this feature to run arbitrary executable for code execution and privilege escalation. Remove the compiler option -rpath to remove @rpath.
CODE SIGNATURE	True	info	This binary has a code signature.
ENCRYPTED	False	warning	This binary is not encrypted.
SYMBOLS STRIPPED	False	warning	Symbols are available. To strip debugging symbols, set Strip Debug Symbols During Copy to YES, Deployment Postprocessing to YES, and Strip Linked Product to YES in project's build settings.

Q DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
googleads.g.doubleclick.net	ok	IP: 142.250.74.34 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
admob-gmats.uc.r.appspot.com	ok	IP: 216.58.211.20 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
crl.apple.com	ok	IP: 17.253.39.206 Country: Sweden Region: Stockholms lan City: Stockholm Latitude: 59.332581 Longitude: 18.064899 View: Google Map
www.apple.com	ok	IP: 23.199.248.211 Country: United States of America Region: Texas City: Dallas Latitude: 32.783058 Longitude: -96.806671 View: Google Map

DOMAIN	STATUS	GEOLOCATION
www.google.com	ok	IP: 142.250.74.100 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
app-measurement.com	ok	IP: 142.250.74.174 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
developer.android.com	ok	IP: 142.250.74.14 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
.app-measurement.com	ok	No Geolocation information available.
www.googleadservices.com	ok	IP: 142.250.74.162 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

DOMAIN	STATUS	GEOLOCATION
pagead2.googlesyndication.com	ok	IP: 142.250.74.98 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
csi.gstatic.com	ok	IP: 142.250.111.120 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
dl.google.com	ok	IP: 142.250.74.14 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
googlemobileadssdk.page.link	ok	IP: 142.250.74.142 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

DOMAIN	STATUS	GEOLOCATION
play.googleapis.com	ok	IP: 142.250.74.138 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
firebaseml.googleapis.com	ok	IP: 142.250.74.170 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
firebaseremoteconfig.googleapis.com	ok	IP: 142.250.74.170 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
www.leptonica.com	ok	IP: 142.250.74.83 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

DOMAIN	STATUS	GEOLOCATION
fundingchoicesmessages.google.com	ok	IP: 172.217.21.174 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
firebaseinstallations.googleapis.com	ok	IP: 216.58.211.10 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
ocsp.apple.com	ok	IP: 17.253.39.202 Country: Sweden Region: Stockholms lan City: Stockholm Latitude: 59.332581 Longitude: 18.064899 View: Google Map
badad.googleplex.com	ok	IP: 142.251.1.129 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
ns.adobe.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
imasdk.googleapis.com	ok	IP: 172.217.21.170 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
www.w3.org	ok	IP: 128.30.52.100 Country: United States of America Region: Massachusetts City: Cambridge Latitude: 42.365078 Longitude: -71.104523 View: Google Map
symbolize.corp.google.com	ok	IP: 173.194.222.129 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
jmt17.google.com	ok	IP: 172.217.21.174 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

DOMAIN	STATUS	GEOLOCATION
support.google.com	ok	IP: 142.250.74.142 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
google.com	ok	IP: 142.250.74.78 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
goo.gl	ok	IP: 142.250.74.174 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
www.googleapis.com	ok	IP: 142.250.74.10 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

DOMAIN	STATUS	GEOLOCATION
github.com	ok	IP: 140.82.121.3 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map

EMAILS

EMAIL	FILE
_@7.ogs i.@j.aj 6@z.ĕc 6@s.ĕ9h 6w@o.ĕz 6@f.ĕ9h &i@lt3.c3n tj@i.eyp jsteffens@google.com sales@nevenvision.com filesarray.@min.local 0@153□q56٩vl □@mb.mfsp 9@s.js i@i.najf 1t@v.p@ 21lv@7hyka.67v z3@k.mmzbg x8@□aj.guv9	Runner.app/Runner

EMAIL	FILE
dn@snden.hhh	Runner.app/GoogleMVTextDetectorResources.bundle/tflite_langid.tflite
v@w.09 3n@b.r3q a@6.6e 2@-3mö.9g n@4b.dmq8 d@2g.x7cdb be0@86.bx 64m@k7o.o8y49 pt@nu.884n ewj@f6.ǯcieh dc2@5b.w45 hu@80.q5 -b@aid.pn xnfk@r.9q 2@a88.cd r12@3pd.8a b@2b.g8 -@3.c9 9@z.1j g2□rd@h.hrhľc2eiqc a5fiah@hhh7.yţ ml@hlo.p8j n@jmol.evȟxi u@h.ijh e3i@ĭe.hwgd dii@bv.h8 acy@s9šl.fom a@ky5r_i.m4 kb@dil.kdgme dl@zt.lb	Runner.app/MLKitPoseDetectionAccurateResources.bundle/pose_landmark_detector_accurate.tflite

EMAIL	FILE
ťg9@ťiej.fwx c@z.bd x19a6f4vbbm.@di.8àfd	Runner.app/MLKitPoseDetectionAccurateResources.bundle/pose_person_detector_accurate.tflite
uy@at.l8yz o@ddugjhgm.6cdkkeu miafs0tuu@z.xl xkd@jkfpefqymui.aj2 hhkhalq@xlh.qy urxgk@t.cfrnv ee@_s.nusutonacv	Runner.app/GoogleMVFaceDetectorResources.bundle/fssd_100_8bit_v1.tflite
nnfi0eachhfil71ap@qnncnabkfvcu.ufbj6grq5g e3i_uho@_xqxpjl.inue 6@81775.f8 o_l@4.o1y_im9oai c@alek.gega lixsjjlj@ie.dvamihn7jx v@xwwr.blf f@b9tdr8ebfaed.mhnq exzph@xq.njw r@f.miy ajgri-sdrpbgaqfoo7@eepyxnf.qu l_6@xvtiqxxcagz.yyjl	Runner.app/GoogleMVFaceDetectorResources.bundle/fssd_100_8bit_gray_v1.tflite
5c@gtztcw.zy5cuncetd af@a.aa	Runner.app/GoogleMVFaceDetectorResources.bundle/fssd_25_8bit_v1.tflite
ebwpgeudclwicjq8gaod@ihf.ljgszofy	Runner.app/GoogleMVFaceDetectorResources.bundle/fssd_25_8bit_gray_v1.tflite

EMAIL	FILE
8-@nv.06 r@db.6x8 Br8b@2.l2q r@7\$.b8 4@8.44 ac@n.ùb i@6fe7.5p u'@dģ9d.6prcp 4_@r.0t0 kl940@u6p.18 0@j.98 w39@ah.690s b@k.0\frace 5@015.yu ag86@2ad.gc d@_h.ģe 3@c.8i	Runner.app/MLKitPoseDetectionFastResources.bundle/pose_landmark_detector_fast.tflite
ťg9@ťiej.fwx c@z.bd x19a6f4vbbm.@di.8àfd	Runner.app/MLKitPoseDetectionFastResources.bundle/pose_person_detector_fast.tflite
ed@d7.mr	Runner.app/MLKitObjectDetectionCommonResources.bundle/tflite_mobile_object_localizer_3_1.tflite
tj@i.eyp 9@s.js sales@nevenvision.com i@lt3.c3n z3@k.mmzbg 21lv@7hyka.67v i.@j.aj jsteffens@google.com i@i.najf 0@153 filesarray.@min.local	IPA Strings Dump



TRACKER	CATEGORIES	URL
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google DoubleClick		https://reports.exodus-privacy.eu.org/trackers/5

APP STORE INFORMATION

Title: GreenPass Italia

Score: 4.87155 Features: iosUniversal, Price: 0.0 Category: Utilities, Medical,

App Store URL: com.italinnovation.greenPass

Developer: Ital Innovation SRL **Developer ID:** 1510586898 **Developer Website:** https://iisrl.it

Developer URL: https://apps.apple.com/us/developer/ital-innovation-srl/id1510586898?uo=4

Supported Devices iPhone5s-iPhone5s, iPadAir-iPadAir, iPadAirCellular-iPadAirCellular, iPadMiniRetina, iPadMiniRetina, iPadMiniRetinaCellular-iPadMiniRetinaCellular, iPhone6-iPhone6, iPhone6Plus-iPhone6Plus, iPadAir2-iPadAir2, iPadAir2Cellular-iPadAir2Cellular, iPadMini3-iPadMini3, iPadMini3Cellular-iPadMini3Cellular, iPodTouchSixthGen.iPhone6SiPhone6s, iPhone6sPlus-iPhone6sPlus, iPadMini4-iPadMini4, iPadMini4Cellular-iPadMini4Cellular, iPadMini4Cellular, iPadMini4Cellular-iPadMini4Cellular, iPadMini4Cellular-iPadMini4Cellular, iPadMini4Cellular, iPadMini5Cellular, iPadMini5Cellular, iPadMini5Cellular, iPadMini5Cellular, iPadMini5Cellular, iPadMini5Cellular, iPadMini5Cellular, iPadMini5Cellular, iPadMini5Cellular, iPadMini4Cellular, iPadProFithGen-iPadProSecondGen-iP

Description:

QUEST'APPLICAZIONE NON PERMETTE DI SCARICARE IL GREEN PASS In questa applicazione potrai salvare tutti i GreenPass che hai bisogno di avere sempre a portata di mano, che siano tuoi o dei tuoi familiari. Potrai scannerizzare il QRcode e salvarlo in modo da poterlo utilizzare facilmente tutte le volte che ti verrà richiesto. Con le nuove normative sarà obbligatorio mostrarlo all'ingresso di alcune attività aperte al pubblico e con questa applicazione non dovrai più preoccuparti di andarlo a cercare tra mille altre immagini. I dati del tuo GreenPass verranno salvati solamente all'interno del tuo telefono e non saranno accessibili né a noi né a chiunque altro. Questo per garantire il rispetto della tua privacy e per una maggiore sicurezza dei dati. La nostra società si occupa della creazione di prodotti digitali, per maggiori informazioni contattaci a info@iisrl.it

Report Generated by - MobSF v3.5.1 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.

© 2022 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.