



IOS STATIC ANALYSIS REPORT

app_icon

 GreenCheck (1.18)

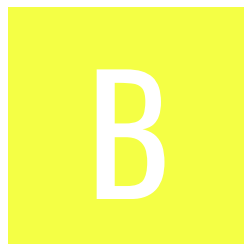
File Name: GreenCheck.ipa

Identifier: at.itsv.mobile.cochap





Scan Date: May 7, 2022, 12:47 p.m.

App Security Score: 44/100 (MEDIUM RISK)

Grade:



FINDINGS SEVERITY

 HIGH	 WARNING	 INFO	 SECURE
2	2	2	1

FILE INFORMATION

File Name: GreenCheck.ipa

Size: 2.73MB

MD5: a94bddac182b1ccd6364802cf00a911c

SHA1: 858878066fc556eec6327860e861c1c43dccffa5

SHA256: 8eae8110e44414b16155eb09b9db11238a39b46b014250939b110e7d9948384

APP INFORMATION

App Name: GreenCheck

App Type: Objective C

Identifier: at.itsv.mobile.cochap

SDK Name: iphoneos15.2

Version: 1.18

Build: 251

Platform Version: 15.2

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.	GreenCheck benötigt Zugriff auf die Kamera, um QR-Codes scannen zu können.

🔒

APP TRANSPORT SECURITY (ATS)

NO	ISSUE	SEVERITY	DESCRIPTION
1	NSExceptionDomains	info	localhost

</>

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) <code>_printf</code> , <code>_strncat</code> , <code>_sscanf</code> , <code>_strcpy</code> , <code>_vsprintf</code> , <code>_stat</code> , <code>_memcpy</code> , <code>_fopen</code> , <code>_strlen</code>
2	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 <code>_NSLog</code> function for logging.
3	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 <code>_malloc</code> function instead of <code>calloc</code>

IPA BINARY ANALYSIS

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 <code>-fPIC</code> 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.

PROTECTION	STATUS	SEVERITY	DESCRIPTION
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.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
gruenerpass.gv.at	ok	IP: 194.48.236.195 Country: Austria Region: Wien City: Vienna Latitude: 48.208488 Longitude: 16.372080 View: Google Map

DOMAIN	STATUS	GEOLOCATION
phrogz.net	ok	IP: 69.46.18.236 Country: United States of America Region: Florida City: Tampa Latitude: 28.007360 Longitude: -82.515450 View: Google Map
webkit.org	ok	IP: 54.190.50.171 Country: United States of America Region: Oregon City: Portland Latitude: 45.523449 Longitude: -122.676208 View: Google Map
crl.apple.com	ok	IP: 17.253.39.202 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
raw.githubusercontent.com	ok	IP: 185.199.111.133 Country: United States of America Region: Pennsylvania City: California Latitude: 40.065632 Longitude: -79.891708 View: Google Map
greencheck.gv.at	ok	IP: 157.177.248.43 Country: Austria Region: Wien City: Vienna Latitude: 48.208488 Longitude: 16.372080 View: Google Map
react-native-async-storage.github.io	ok	IP: 185.199.108.153 Country: United States of America Region: Pennsylvania City: California Latitude: 40.065632 Longitude: -79.891708 View: Google Map
drafts.csswg.org	ok	IP: 173.230.149.95 Country: United States of America Region: California City: Fremont Latitude: 37.548271 Longitude: -121.988571 View: Google Map

DOMAIN	STATUS	GEOLOCATION
www.itsv.at	ok	IP: 212.183.22.3 Country: Austria Region: Wien City: Vienna Latitude: 48.208488 Longitude: 16.372080 View: Google Map
help.dottoro.com	ok	IP: 66.228.34.81 Country: United States of America Region: New Jersey City: Cedar Knolls Latitude: 40.821945 Longitude: -74.448891 View: Google Map
git.io	ok	IP: 140.82.113.21 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
css-infos.net	ok	IP: 213.186.33.4 Country: France Region: Hauts-de-France City: Roubaix Latitude: 50.694210 Longitude: 3.174560 View: Google Map

DOMAIN	STATUS	GEOLOCATION
reactnavigation.org	ok	IP: 162.159.137.85 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
ocsp.apple.com	ok	IP: 17.253.39.203 Country: Sweden Region: Stockholms lan City: Stockholm Latitude: 59.332581 Longitude: 18.064899 View: Google Map
docs.swmansion.com	ok	IP: 104.21.27.136 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
reactjs.org	ok	IP: 76.76.21.21 Country: United States of America Region: California City: Walnut Latitude: 34.015400 Longitude: -117.858223 View: Google Map

DOMAIN	STATUS	GEOLOCATION
drafts.fxtf.org	ok	IP: 23.92.26.181 Country: United States of America Region: California City: Fremont Latitude: 37.548271 Longitude: -121.988571 View: Google Map
developer.mozilla.org	ok	IP: 108.156.22.4 Country: United States of America Region: Washington City: Redmond Latitude: 47.682899 Longitude: -122.120903 View: Google Map
msdn.microsoft.com	ok	IP: 13.107.246.44 Country: Netherlands Region: Noord-Holland City: Amsterdam Latitude: 52.374031 Longitude: 4.889690 View: Google Map
bugzilla.mozilla.org	ok	IP: 35.167.131.119 Country: United States of America Region: Oregon City: Portland Latitude: 45.523449 Longitude: -122.676208 View: Google Map

DOMAIN	STATUS	GEOLOCATION
callstack.github.io	ok	IP: 185.199.111.153 Country: United States of America Region: Pennsylvania City: California Latitude: 40.065632 Longitude: -79.891708 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
www.sozialministerium.at	ok	IP: 95.131.199.37 Country: Austria Region: Wien City: Vienna Latitude: 48.208488 Longitude: 16.372080 View: Google Map
www.sitepoint.com	ok	IP: 108.156.22.18 Country: United States of America Region: Washington City: Redmond Latitude: 47.682899 Longitude: -122.120903 View: Google Map

DOMAIN	STATUS	GEOLOCATION
example.com	ok	IP: 93.184.216.34 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
cssdot.ru	ok	IP: 95.216.245.81 Country: Finland Region: Uusimaa City: Helsinki Latitude: 60.169521 Longitude: 24.935450 View: Google Map
github.com	ok	IP: 140.82.121.4 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
fb.me	ok	IP: 31.13.72.36 Country: Sweden Region: Stockholms lan City: Stockholm Latitude: 59.332581 Longitude: 18.064899 View: Google Map

DOMAIN	STATUS	GEOLOCATION
stackoverflow.com	ok	IP: 151.101.1.69 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
json-schema.org	ok	IP: 104.21.8.16 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map

EMAILS

EMAIL	FILE
m@v.wo1	GreenCheck.app/GreenCheck
rdvornov@gmail.com post@sozialministerium.at dsb@dsb.gv datenschutz@greencheck.gv	GreenCheck.app/main.jsbundle
rdvornov@gmail.com	GreenCheck.app/assets/node_modules/css-tree/package.json
m@v.wo1	IPA Strings Dump

EMAIL	FILE
-------	------

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](#).