



ANDROID STATIC ANALYSIS REPORT



 Places App (1.0-beta12)

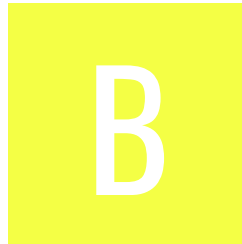
File Name: AccessApp Places_1.0-beta12_apkcombo.com (1).apk

Package Name: app.downloadaccess.places

Scan Date: March 14, 2022, 9:36 p.m.






App Security Score: 53/100 (MEDIUM RISK)

Grade:



Trackers Detection: 2/421

FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
1	4	1	1	1

FILE INFORMATION

File Name: AccessApp Places_1.0-beta12_apkcombo.com (1).apk

Size: 5.33MB

MD5: b8247f23be6d59860cc8bea47eb8d845

SHA1: d27ed1dde095056d206c9b174c1af59fccc5dc27

SHA256: 6caab8365bf230fdc73a1997c4e37e57fdaace6e4c85f847c35cd3ed6d371340

APP INFORMATION

App Name: Places App

Package Name: app.downloadaccess.places

Main Activity: app.downloadaccess.places.MainActivity

Target SDK: 29

Min SDK: 23

Max SDK:

Android Version Name: 1.0-beta12

Android Version Code: 5

APP COMPONENTS

Activities: 2

Services: 3

Receivers: 1

Providers: 2

Exported Activities: 0

Exported Services: 0

Exported Receivers: 0

Exported Providers: 0

CERTIFICATE INFORMATION

APK is signed

v1 signature: True

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: 2020-09-18 09:54:52+00:00

Valid To: 2050-09-18 09:54:52+00:00

Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android

Serial Number: 0x1d11984c5fd1cffa32040fee893ba397dc46ee56

Hash Algorithm: sha256

md5: 6617c14b414b42551f0025fbca014725

sha1: fbdb94e4dfff3a6fd199f54fc7ae5ea70d135ddb

sha256: a9f5ee63ee1195d16f34801907795cef9f80b0941c50e3ccff0e8144a0531a60

sha512: 894d9ec152ce73f080c112843d362e862ee48e2d733c96059db9c626aa9450d6f7397364ff42a8038dc96504e299d9e1ae584a51cc94e9ab6cfd237c3bb01c00

PublicKey Algorithm: rsa

Bit Size: 4096

Fingerprint: bd38aefb3174caf928329db7a4dc0dc788e9aaa2de26ad02605b2eee0daa2f3f

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	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.INTERNET	normal	full Internet access	Allows an application to create network sockets.
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.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.

APKID ANALYSIS

FILE	DETAILS
------	---------

FILE	DETAILS	
classes.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.TAGS check possible VM check
	Anti Debug Code	Debug.isDebuggerConnected() check
	Compiler	r8
classes2.dex	FINDINGS	DETAILS
	Compiler	r8 without marker (suspicious)

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	high	Base config is insecurely configured to permit clear text traffic to all domains.

Q MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_sec_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.

</> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	app/downloadaccess/places/navigation/child/PlaceInfoFragment.java app/downloadaccess/places/navigation/child/PlacesFragment.java app/downloadaccess/resources/Utils.java app/downloadaccess/places/navigation/child/AddPlaceFragment.java app/downloadaccess/places/MainActivity.java app/downloadaccess/places/navigation/PlacesFragmentContainer.java
2	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	io/jsonwebtoken/JwsHeader.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	app/downloadaccess/resources/network/RetrofitClientInstance.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_RBG_EXT.1.1	Security Functional Requirements	Random Bit Generation Services	The application invoke platform-provided DRBG functionality for its cryptographic operations.
2	FCS_STO_EXT.1.1	Security Functional Requirements	Storage of Credentials	The application does not store any credentials to non-volatile memory.
3	FCS_CKM_EXT.1.1	Security Functional Requirements	Cryptographic Key Generation Services	The application implement asymmetric key generation.
4	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['camera', 'network connectivity'].
5	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to no sensitive information repositories.
6	FDP_NET_EXT.1.1	Security Functional Requirements	Network Communications	The application has user/application initiated network communications.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
7	FDP_DAR_EXT.1.1	Security Functional Requirements	Encryption Of Sensitive Application Data	The application implement functionality to encrypt sensitive data in non-volatile memory.
8	FMT_MEC_EXT.1.1	Security Functional Requirements	Supported Configuration Mechanism	The application invoke the mechanisms recommended by the platform vendor for storing and setting configuration options.
9	FTP_DIT_EXT.1.1	Security Functional Requirements	Protection of Data in Transit	The application does encrypt some transmitted data with HTTPS/TLS/SSH between itself and another trusted IT product.
10	FCS_RBG_EXT.2.1,FCS_RBG_EXT.2.2	Selection-Based Security Functional Requirements	Random Bit Generation from Application	The application perform all deterministic random bit generation (DRBG) services in accordance with NIST Special Publication 800-90A using Hash_DRBG. The deterministic RBG is seeded by an entropy source that accumulates entropy from a platform-based DRBG and a software-based noise source, with a minimum of 256 bits of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.
11	FCS_CKM.1.1(1)	Selection-Based Security Functional Requirements	Cryptographic Asymmetric Key Generation	The application generate asymmetric cryptographic keys not in accordance with FCS_CKM.1.1(1) using key generation algorithm RSA schemes and cryptographic key sizes of 1024-bit or lower.
12	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.
13	FCS_HTTPS_EXT.1.3	Selection-Based Security Functional Requirements	HTTPS Protocol	The application notify the user and not establish the connection or request application authorization to establish the connection if the peer certificate is deemed invalid.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
14	FIA_X509_EXT.2.1	Selection-Based Security Functional Requirements	X.509 Certificate Authentication	The application use X.509v3 certificates as defined by RFC 5280 to support authentication for HTTPS , TLS.
15	FPT_TUD_EXT.2.1	Selection-Based Security Functional Requirements	Integrity for Installation and Update	The application shall be distributed using the format of the platform-supported package manager.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
access-app-aux.firebaseio.com	ok	IP: 35.201.97.85 Country: United States of America Region: Missouri City: Kansas City Latitude: 39.099731 Longitude: -94.578568 View: Google Map
www.centralpark.com	ok	IP: 75.101.132.169 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map

DOMAIN	STATUS	GEOLOCATION
downloadaccess.app	ok	IP: 3.125.252.47 Country: Germany Region: Hessen City: Frankfurt am Main Latitude: 50.115520 Longitude: 8.684170 View: Google Map
tools.ietf.org	ok	IP: 64.170.98.42 Country: United States of America Region: New York City: New York City Latitude: 40.714272 Longitude: -74.005966 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

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://access-app-aux.firebaseio.com	info App talks to a Firebase Database.

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://access-app-aux.firebaseio.com"
"google_api_key" : "AlzaSyB3Pn64KvgJlDvpjH319GrXONm_StL9J9Q"
"google_crash_reporting_api_key" : "AlzaSyB3Pn64KvgJlDvpjH319GrXONm_StL9J9Q"

PLAYSTORE INFORMATION

Title: AccessApp Places

Score: None **Installs:** 1+ **Price:** 0 **Android Version Support:** Varies with device **Category:** Events **Play Store URL:** [app.downloadaccess.places](https://play.google.com/store/apps/details?id=com.aux.accessapp.places)

Developer Details: AuxCode, AuxCode, Vasil Kirkov 19 1164 Sofia Bulgaria, <https://downloadplaces.app>, t.e.shaw@auxnederlandbv.nl,

Release Date: None **Privacy Policy:** [Privacy link](#)

Description:

AccessApp Places allows Managers of Places to add and edit Places.

Report Generated by - MobSF v3.5.2 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](#).