MOBSF

ANDROID STATIC ANALYSIS REPORT

2FA Authenticator (1.0)

File Name:	com.privacy.account.safetyapp_10_apksos.com.apk
Package Name:	com.privacy.account.safetyapp
Scan Date:	May 22, 2022, 1:44 p.m.
App Security Score:	51/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	10	2	1	1

FILE INFORMATION

File Name: com.privacy.account.safetyapp_10_apksos.com.apk
Size: 3.53MB
MD5: f02b43edca6f52926a99145572b64b98
SHA1: e05c2784c71fafc3f8d95077d419c99bc4770de5
SHA256: 11558904bb5a8ae28100dd6f139f31c837411d56adfae6a0c3d4d980e7fb8953

APP INFORMATION

App Name: 2FA Authenticator
Package Name: com.privacy.account.safetyapp
Main Activity: com.privacy.account.safetyapp.ui.MainActivity
Target SDK: 30
Min SDK: 26
Max SDK:
Android Version Name: 1.0
Android Version Code: 1

APP COMPONENTS

Activities: 14
Services: 2
Receivers: 1
Providers: 2
Exported Activities: 1
Exported Services: 0
Exported Receivers: 1
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: 2022-01-12 21:07:09+00:00
Valid To: 2052-01-12 21:07:09+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xef7c7b00f9d1defaf7b7f39af90decc9f7edff6e
Hash Algorithm: sha256
md5: aea2f0271fe3e0ed92e92fb82abdbd21
sha1: 9fd796701fa65066a64b14da912350050fcf3ffb
sha256: 69e501ae17c5d8893d86adaa3261129538be084914a6f618d68d2d19a219d1ef
sha512: 5b06b5b0c86573aed3636131406c4658e57d624e8e6c5ae9c49f4a821d831c39a0d4ec1a2b518cd6ee8dc0c73288f8ad3d2e778e8d87fde716ed876551cad4d0
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 2626ab53333c368c1b73d8131162ebb51e616781c7011ed969efee39ed70af43

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
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.QUERY_ALL_PACKAGES	normal		Allows query of any normal app on the device, regardless of manifest declarations.
android.permission.SYSTEM_ALERT_WINDOW	dangerous	display system-level alerts	Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.
android.permission.REQUEST_INSTALL_PACKAGES	dangerous	Allows an application to request installing packages.	Malicious applications can use this to try and trick users into installing additional malicious packages.
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.

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.DISABLE_KEYGUARD	normal		Allows applications to disable the keyguard if it is not secure.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.USE_BIOMETRIC	normal		Allows an app to use device supported biometric modalities.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check Build.MANUFACTURER check FINDINGS: Compiler — DETAILS: r8

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.privacy.account.safetyapp.ui.MainActivity	Schemes: otpauth://, Mime Types: image/*,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
2	Broadcast Receiver (org.hamcrest.BootBroadcastReceiver) is not Protected. An intent-filter exists.	warning	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	Activity (com.privacy.account.safetyapp.ui.PanicResponderActivity) is not Protected. An intent-filter exists.	warning	An Activity 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 Activity is explicitly exported.
4	High Intent Priority (10000) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.

NO	ISSUE	SEVERITY	DESCRIPTION

</> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
				b/i/b/h/e.java c/d/a/q/t/o/b.java b/k/l/b.java c/d/a/q/t/b.java c/d/a/q/w/a.java b/b/p/i/g.java b/b/q/g1.java b/b/q/t.java c/d/a/q/w/d/b0.java b/p/d/l.java b/b/q/w0.java c/e/a/g.java c/e/a/h.java c/d/a/q/v/c.java b/b/p/i/d.java b/d/s.java c/d/a/r/e.java c/d/a/q/u/c0/j.java b/u/e/l.java c/d/a/q/u/d0/j.java c/d/a/r/o.java b/b/k/s.java b/d/p.java c/d/a/q/w/h/a.java b/b/q/x0.java b/p/d/i0.java

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	c/e/a/b.java b/b/k/p.java b/k/l/z.java b/p/d/a0.java c/f/a/a/a0/e0.java c/d/a/r/s.java c/d/a/q/w/h/d.java com/bumptech/glide/GeneratedAppGlideModuleImpl.java b/p/d/j0.java b/p/d/x0.java b/i/b/d.java c/d/a/r/p.java b/e/b/k1.java b/b/q/m0.java c/g/a/e/a.java b/p/d/c.java b/b/k/c0.java c/d/a/q/u/j.java c/d/a/o/d.java b/b/q/g0.java c/d/a/q/w/d/z.java c/d/a/u/j/j.java b/b/q/s0.java b/b/p/f.java b/m/b/e.java c/d/a/q/u/b0.java c/d/a/q/u/c0/i.java c/d/a/l.java c/g/a/e/b.java c/g/a/a.java c/d/a/q/w/d/r.java c/d/a/q/v/s.java b/p/d/a.java b/k/h/c.java b/t/j.java b/n/a/b.java com/privacy/account/safetyapp/ui/AuthActivity.java b/k/l/p.java b/p/d/y0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				b/l/a/b.java b/k/e/d.java c/d/a/q/w/d/m.java b/b/q/o0.java c/d/a/k.java c/d/a/q/u/i.java c/d/a/q/w/d/k.java b/b/q/x.java c/d/a/u/h.java b/i/c/d.java b/d/j.java c/h/a/j/f.java c/f/a/a/l/g.java c/d/a/q/u/d0/e.java b/k/c/c.java c/d/a/q/t/l.java c/d/a/q/v/t.java b/k/m/e.java c/d/a/o/e.java c/f/a/a/c0/b.java b/b/q/c0.java c/i/a/a/r/j.java b/d/t.java c/d/a/q/u/r.java c/d/a/q/u/e0/a.java b/i/c/c.java b/p/d/c0.java c/e/a/j.java b/e/a/b/s0.java b/k/c/h.java c/f/a/a/d0/a.java c/d/a/u/j/d.java b/o/a/a.java c/d/a/q/w/h/j.java b/k/k/a.java b/k/c/b.java b/b/q/k.java b/d/u.java c/d/a/q/w/d/n.java b/k/e/e.java c/d/a/w/l/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				b/p/d/m.java c/d/a/q/t/j.java b/i/c/b.java c/d/a/c.java b/k/l/a.java c/d/a/q/w/d/c.java c/f/a/a/f0/g.java c/h/a/k/b.java c/j/a/c/w.java b/p/d/f0.java b/b/q/e1.java b/k/l/h.java com/privacy/account/safetyapp/ui/PanicResponderActivity.java c/d/a/q/v/d.java com/privacy/account/safetyapp/ui/views/EntryListView.java b/w/b0.java c/d/a/q/v/f.java c/d/a/q/u/l.java b/a/g/d.java b/d/e.java
2	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	c/a/a/b/a.java b/a/g/d.java
3	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	b/d/s.java com/privacy/account/safetyapp/importers/TotpAuthenticatorImporter.java com/privacy/account/safetyapp/importers/AuthyImporter.java
4	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	com/privacy/account/safetyapp/importers/TotpAuthenticatorImporter.java c/d/a/q/u/q.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	com/privacy/account/safetyapp/ui/AboutActivity.java com/privacy/account/safetyapp/ui/ImportEntriesActivity.java com/privacy/account/safetyapp/ui/MainActivity.java c/f/a/a/a0/i0.java
6	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	c/i/a/a/p/g1/b.java com/privacy/account/safetyapp/ui/fragments/ImportExportPreferencesFragment.java c/i/a/a/p/g1/c.java c/i/a/a/r/j.java com/privacy/account/safetyapp/importers/SqlImporterHelper.java
7	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/privacy/account/safetyapp/importers/AuthyImporter.java com/privacy/account/safetyapp/importers/AndOtpImporter.java
8	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/privacy/account/safetyapp/importers/SqlImporterHelper.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 generate no asymmetric cryptographic keys.
4	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['network connectivity', 'camera'].
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.
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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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(3),FCS_CKM.1.2(3)	Selection-Based Security Functional Requirements	Password Conditioning	A password/passphrase shall perform [Password-based Key Derivation Functions] in accordance with a specified cryptographic algorithm..
12	FCS_COP.1.1(1)	Selection-Based Security Functional Requirements	Cryptographic Operation - Encryption/Decryption	The application perform encryption/decryption in accordance with a specified cryptographic algorithm AES-CBC (as defined in NIST SP 800-38A) mode or AES-GCM (as defined in NIST SP 800-38D) and cryptographic key sizes 256-bit/128-bit.
13	FCS_COP.1.1(2)	Selection-Based Security Functional Requirements	Cryptographic Operation - Hashing	The application perform cryptographic hashing services in accordance with a specified cryptographic algorithm SHA-1/SHA-256/SHA-384/SHA-512 and message digest sizes 160/256/384/512 bits.
14	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.
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.
16	FCS_CKM.1.1(2)	Optional Security Functional Requirements	Cryptographic Symmetric Key Generation	The application shall generate symmetric cryptographic keys using a Random Bit Generator as specified in FCS_RBG_EXT.1 and specified cryptographic key sizes 128 bit or 256 bit.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
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
play.google.com	ok	**IP:** 142.251.36.46 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
mikepenz.com	ok	**IP:** 172.67.141.197 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
xml.org	ok	**IP:** 104.239.240.11 **Country:** United States of America **Region:** Texas **City:** Windcrest **Latitude:** 29.499678 **Longitude:** -98.399246 **View:** Google Map
zavoloklom.github.io	ok	**IP:** 185.199.109.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
scripts.sil.org	ok	**IP:** 104.22.10.254 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
psdev.de	ok	**IP:** 49.12.32.214 **Country:** Germany **Region:** Sachsen **City:** Falkenstein **Latitude:** 50.477879 **Longitude:** 12.371290 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
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
xmlpull.org	ok	**IP:** 74.50.61.58 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.814899 **Longitude:** -96.879204 **View:** Google Map
ns.adobe.com	ok	No Geolocation information available.

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"authentication_method_password" : "Password"
"authentication_method_set_password" : "Password"
"choose_authentication_method" : "Security"
"library_AndroidIconics_authorWebsite" : "http://mikepenz.com/"

POSSIBLE SECRETS
"library_MaterialDesignIconicIcons_authorWebsite" : "http://zavoloklom.github.io/material-design-iconic-font"
"password" : "Password"
"secret" : "Secret"

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.