MOBSF

ANDROID STATIC ANALYSIS REPORT

SyncPlayer (1.6.4)

File Name:	installer226.apk
Package Name:	io.github.powerinside.syncplay
Scan Date:	May 31, 2022, 2:16 p.m.
App Security Score:	61/100 (LOW RISK)
Grade:	A

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
0	5	1	1	1

FILE INFORMATION

File Name: installer226.apk
Size: 1.42MB
MD5: 3293020779224951f0c51183586a7b6a
SHA1: 736c7d7f061b82e4cd611ae518ae318e73e2b62e
SHA256: 2d74e8d18a15eefe71f2d23c33204b6ad5f7891bbb09fcf9657bfa49445c7a18

APP INFORMATION

App Name: SyncPlayer
Package Name: io.github.powerinside.syncplay
Main Activity: io.github.powerinside.syncplay.MainActivity
Target SDK: 25
Min SDK: 14
Max SDK:
Android Version Name: 1.6.4
Android Version Code: 18

APP COMPONENTS

Activities: 4
Services: 1
Receivers: 0
Providers: 0
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: False
Found 1 unique certificates
Subject: C=IN, ST=Kerala, L=Calicut, CN=Mohammed Irfan
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2016-04-16 04:39:50+00:00
Valid To: 2041-04-10 04:39:50+00:00
Issuer: C=IN, ST=Kerala, L=Calicut, CN=Mohammed Irfan
Serial Number: 0x3f112445
Hash Algorithm: sha256
md5: fce33595509515d6505bb113055f8084
sha1: d5edca8128ca2e3b17d6bfd6a753d56e4d251569
sha256: def6f9f885e8656d271f5c79428d3a132ec5893f1d6e51caf033f608717bb68c
sha512: 677faa7adc5babb4cfcb6017f75cc9938fb1613151c099751d93206ca945a806c7f60d7ca682b1a7648b817f99133e9220ef4a6cf25def22be247648a428646c
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: e90facf87a32509a32f3aeb1518add92b0520e6deb7bef55544bf942ff7e5e3e

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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.

APKID ANALYSIS

FILE	DETAILS

FILE	DETAILS
classes.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check</td></tr><tr><td>Compiler</td><td>dx</td></tr></table>

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.

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	io/github/powerinside/syncplay/MediaService.java a/a/a/a/a.java
2	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	io/github/powerinside/syncplay/a/a.java
3	MD5 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/a/a/c.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_STO_EXT.1.1	Security Functional Requirements	Storage of Credentials	The application does not store any credentials to non-volatile memory.
2	FCS_CKM_EXT.1.1	Security Functional Requirements	Cryptographic Key Generation Services	The application generate no asymmetric cryptographic keys.
3	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['network connectivity'].

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
4	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to no sensitive information repositories.
5	FDP_NET_EXT.1.1	Security Functional Requirements	Network Communications	The application has user/application initiated network communications.
6	FDP_DAR_EXT.1.1	Security Functional Requirements	Encryption Of Sensitive Application Data	The application does not encrypt files in non-volatile memory.
7	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.
8	FTP_DIT_EXT.1.1	Security Functional Requirements	Protection of Data in Transit	The application does not encrypt any data in traffic or does not transmit any data between itself and another trusted IT product.
9	FCS_COP.1.1(2)	Selection-Based Security Functional Requirements	Cryptographic Operation - Hashing	The application perform cryptographic hashing services not in accordance with FCS_COP.1.1(2) and uses the cryptographic algorithm RC2/RC4/MD4/MD5.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION

DOMAIN	STATUS	GEOLOCATION
www.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
cketti.de	ok	**IP:** 185.199.108.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **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

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"library_ckChangeLog_author" : "cketti"

POSSIBLE SECRETS
"library_ckChangeLog_authorWebsite" : "http://cketti.de/"
"username" : "Nickname"
"username" : "ニックネーム"

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.