

ANDROID STATIC ANALYSIS REPORT



SyncPlayer (1.6.4)

File Name:	installer135.apk
Package Name:	io.github.powerinside.syncplay
Scan Date:	May 31, 2022, 12:37 p.m.
App Security Score:	53/100 (MEDIUM RISK)
Grade:	

FINDINGS SEVERITY

派 HIGH	▲ MEDIUM	i INFO	✓ SECURE	≪ HOTSPOT
1	4	1	1	1

FILE INFORMATION

File Name: installer135.apk

Size: 1.44MB

MD5: bec5cea7b8e44d14a1136bdd4359f682

SHA1: ddf3a47aba1f4cbd96641046d9ad9aa5fcbf212f

SHA256: bc07c2c9618f2026e9ec1a081e9c24b553024717e4c114ca01cc24ba23dbdac1

i APP INFORMATION

App Name: SyncPlayer

Package Name: io.github.powerinside.syncplay

 $\textbf{\textit{Main Activity}}: io. github. power in side. syncplay. Main Activity$

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: O Exported Services: O Exported Receivers: O Exported Providers: O



APK is signed v1 signature: True v2 signature: False v3 signature: False

Found 1 unique certificates

Subject: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid

Signature Algorithm: rsassa_pkcs1v15 Valid From: 2017-05-30 05:10:59+00:00 Valid To: 2044-10-15 05:10:59+00:00

Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid

Serial Number: 0x50902df2 Hash Algorithm: sha256

md5: 79534b1a967d8b11a3969318568a1d87

sha1: 12a24e422f31bfc738d9b3c5187d735a8f80f4d9

sha256: 54aead67b3e715c66f5e940e9858fd89f825c3e869ebd0435fe5106bae697466

sha512: 871de5d14361c4e4844ac5b7b118cab3e15bbf1b2292def4207a87c6db6680eca46b28ff55d3c6c80686c7ef4dc2441c57bd9ec06829a02fc18d10332a6a3027

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

TITLE	SEVERITY	DESCRIPTION
Application vulnerable to Janus Vulnerability	high	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.

M APKID ANALYSIS

FILE	DETAILS

FILE	DETAILS		
	FINDINGS	DETAILS	
I and the second	Anti-VM Code	Build.MANUFACTURER check	
classes.dex	Compiler	dx	

△ NETWORK SECURITY

1	NO	SCOPE	SEVERITY	DESCRIPTION
---	----	-------	----------	-------------

Q 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	a/a/a/a.java io/github/powerinside/syncpla y/MediaService.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/syncpla y/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.

Q 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.

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