# MOBSF

## ANDROID STATIC ANALYSIS REPORT

Protect Baby Monitor (0.3)

| | |
|---|---|
| File Name: | cam2.apk |
| Package Name: | protect.babymonitor |
| Scan Date: | May 23, 2022, 4:59 p.m. |
| App Security Score: | 56/100 (MEDIUM RISK) |
| Grade: | B |

# FINDINGS SEVERITY

| HIGH | MEDIUM | INFO | SECURE | HOTSPOT |
|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 |

# FILE INFORMATION

**File Name:** cam2.apk
**Size:** 0.29MB
**MD5:** 1eae0e69160fb81f3eb3c129cc663301
**SHA1:** 8ccac0e2dfc7334934cb67463e9d440297513489
**SHA256:** d3f663ef2c92ca4015a717b99f8170818a67a14a9ea6b7c92547f9c741598b37

# APP INFORMATION

**App Name:** Protect Baby Monitor
**Package Name:** protect.babymonitor
**Main Activity:** protect.babymonitor.StartActivity
**Target SDK:** 17
**Min SDK:** 16
**Max SDK:**
**Android Version Name:** 0.3
**Android Version Code:** 3

# APP COMPONENTS

Activities: 4
Services: 0
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: 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: 2015-12-29 17:10:25+00:00
Valid To: 2043-05-16 17:10:25+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x2a0388df
Hash Algorithm: sha256
md5: 74c64f3b1da210dbf8781f9917f7968f
sha1: 9b3d060d771df780773a5151baf8b2a8ffa9de0d
sha256: 998a12ba3580c2437ce60e3f111a551de7df1ec29fce86f12857d880838231ff
sha512: 2fc332a6ed97d31ea7139914e38e8f5d93816d60c020a9f153c395e14527370e372ad9a364f1082c62202b48b1c6094a4a1dd5a7e118591025390a78d08ba40d

| 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.RECORD_AUDIO | dangerous | record audio | Allows application to access the audio record path. |
| android.permission.ACCESS_WIFI_STATE | normal | view Wi-Fi status | Allows an application to view the information about the status of Wi-Fi. |

# APKID ANALYSIS

| FILE | DETAILS |
| --- | --- |
| classes.dex | FINDINGS: Compiler — DETAILS: dx (possible dexmerge)<br>FINDINGS: Manipulator Found — DETAILS: dexmerge |

# 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<br>OWASP MASVS: MSTG-STORAGE-3 | protect/babymonitor/StartActivity.java<br>protect/babymonitor/ListenActivity.java<br>protect/babymonitor/DiscoverActivity.java<br>protect/babymonitor/MonitorActivity.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 ['microphone', 'network connectivity']. |
| 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 implement functionality to encrypt sensitive data 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 encrypt some transmitted data with HTTPS/TLS/SSH between itself and another trusted IT product. |

---

## 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.