MOBSF

ANDROID STATIC ANALYSIS REPORT

Protect Baby Monitor (0.3)

File Name:	installer290.apk
Package Name:	protect.babymonitor
Scan Date:	May 31, 2022, 12:21 p.m.
App Security Score:	73/100 (LOW RISK)
Grade:	A

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
0	2	1	1	1

FILE INFORMATION

File Name: installer290.apk
Size: 0.28MB
MD5: 6a17e0b4c4fa9021a0101656e5e7d1ec
SHA1: df53ececa8555734025ec2d31a7a6d332e64abc4
SHA256: 179e891947ecb4b33812674135f853e0599bb556602cc6f04ffbfef69717b858

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: True
v3 signature: False
Found 1 unique certificates
Subject: C=US, ST=KY, L=Lexington, O=None, OU=None, CN=Branden Archer
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2017-03-04 02:40:03+00:00
Valid To: 2044-07-20 02:40:03+00:00
Issuer: C=US, ST=KY, L=Lexington, O=None, OU=None, CN=Branden Archer
Serial Number: 0x7bb56cac
Hash Algorithm: sha256
md5: d06b81ab7a7f5a56f901a35f9b2f4e6f
sha1: 4e6f3ddf4d46c85a6bf01325a411ed0ff8df8ae2
sha256: 2d384f6043758a79b26c3a8a890e43cf02ebce365bdaecedc9a85bf9039bf7ef
sha512: a2df4ee9a531c650aa80612af9800a3018c3f6439e0e3ccbf54ecd8b352840bea71cb6adf820f02d81e4d6507fe2d02d24f78541d2400b943e462eda23ef1dd6
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: a15c21f2c3736e3b344d42631eda55514c8417a52ea5ebbe54d64e16db302970

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.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

FILE	DETAILS
classes.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Compiler</td><td>dx (possible dexmerge)</td></tr><tr><td>Manipulator Found</td><td>dexmerge</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	protect/babymonitor/ListenActivity.java protect/babymonitor/StartActivity.java protect/babymonitor/DiscoverActivity.java 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 ['network connectivity', 'microphone'].
4	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to no sensitive information repositories.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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.