ANDROID STATIC ANALYSIS REPORT

Better Wifi on/off (2.1.0.0)

File Name:	installer45.apk
Package Name:	com.asksven.betterwifionoff
Scan Date:	May 31, 2022, 11:18 a.m.
App Security Score:	39/100 (HIGH RISK)
Grade:	C
Trackers Detection:	1/428

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
3	11	1	0	1

FILE INFORMATION

File Name: installer45.apk
Size: 0.96MB
MD5: 8918bf8d1ffe050fca99a7667769d0b1
SHA1: 120d22cb34799730a734ff171b9bfec9ca9d8ab1
SHA256: cc77dbbe6a567f682fd5307d8e74b4eb7e028a83b82c6a1e38079dea76cf1ac7

APP INFORMATION

App Name: Better Wifi on/off
Package Name: com.asksven.betterwifionoff
Main Activity: .MainActivity
Target SDK: 15
Min SDK: 7
Max SDK:
Android Version Name: 2.1.0.0

Android Version Code: 43

APP COMPONENTS

Activities: 9
Services: 3
Receivers: 6
Providers: 0
Exported Activities: 4
Exported Services: 0
Exported Receivers: 3
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: 2013-12-09 15:54:45+00:00
Valid To: 2041-04-26 15:54:45+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x760d6695
Hash Algorithm: sha256
md5: b06408ff860c8ceef07c38b760697c90
sha1: c5e1937c001745b3934f531531961ba5313b372d
sha256: 886a078b2d160e27dc7f62b34b57fb209709317ae464b6a42cf9bee140899eb5
sha512: 3af90d812ecdbe18a10097c444d61781fd358556d8f5b55dd7cbb9006c238da0cd6d4b5c65f9b93c1c59b5c3201b084c16d0459595a883ac3262f3f6dcc3cc72

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
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.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.CHANGE_WIFI_STATE	normal	change Wi-Fi status	Allows an application to connect to and disconnect from Wi-Fi access points and to make changes to configured Wi-Fi networks.
android.permission.CHANGE_NETWORK_STATE	normal	change network connectivity	Allows applications to change network connectivity state.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.

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.BATTERY_STATS	signature	modify battery statistics	Allows the modification of collected battery statistics. Not for use by common applications.
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.READ_LOGS	dangerous	read sensitive log data	Allows an application to read from the system's various log files. This allows it to discover general information about what you are doing with the phone, potentially including personal or private information.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.

APKID ANALYSIS

FILE	DETAILS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<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>
</td></tr>
</table>

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	Application Data can be Backed up [android:allowBackup] flag is missing.	warning	The flag [android:allowBackup] should be set to false. By default it is set to true and 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.

NO	ISSUE	SEVERITY	DESCRIPTION
2	Activity (com.asksven.betterwifionoff.AppWhitelistActivity) 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.
3	Activity (com.asksven.betterwifionoff.CellLogActivity) 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	Activity (com.asksven.betterwifionoff.TagsActivity) 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.
5	Activity (com.asksven.betterwifionoff.localeplugin.ui.EditActivity) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
6	Broadcast Receiver (com.asksven.betterwifionoff.localeplugin.receiver.FireReceiver) is not Protected. [android:exported=true]	high	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.
7	Broadcast Receiver (.handlers.BroadcastHandler) 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.
8	Broadcast Receiver (MyWidgetProvider) 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.

CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/asksven/android/common/shellutils/Exec.java com/asksven/betterwifionoff/WifiOffAlarmReceiver.java com/asksven/betterwifionoff/utils/WifiControl.java com/asksven/betterwifionoff/MyWidgetProvider.java com/actionbarsherlock/internal/ActionBarSherlockCompat.java com/asksven/android/common/privateapiproxies/BatteryStatsProxy.java com/asksven/betterwifionoff/utils/Configuration.java com/asksven/android/common/utils/StringUtils.java com/actionbarsherlock/widget/SuggestionsAdapter.java com/asksven/betterwifionoff/PluggedWakelock.java com/asksven/android/common/privateapiproxies/Misc.java com/actionbarsherlock/view/MenuInflater.java com/asksven/betterwifionoff/services/UpdateWidgetService.java com/asksven/betterwifionoff/WifiConnectedAlarmReceiver.java com/asksven/android/common/privateapiproxies/NetworkUsage.java com/actionbarsherlock/internal/view/menu/MenuItemImpl.java com/twofortyfouram/locale/BreadCrumber.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	r.java com/actionbarsherlock/internal/nineoldandroids/animation/PropertyValuesHolder.java com/asksven/android/common/utils/GenericLogger.java com/asksven/betterwifionoff/handlers/BroadcastHandler.java com/asksven/betterwifionoff/AppWhitelistActivity.java com/asksven/android/common/privateapiproxies/Wakelock.java com/asksven/android/common/kernelutils/CpuStates.java com/asksven/betterwifionoff/data/AppWhitelistDBHelper.java com/asksven/android/common/privateapiproxies/Alarm.java com/actionbarsherlock/internal/widget/ActionBarView.java com/asksven/andoid/common/contrib/Util.java com/actionbarsherlock/widget/SearchView.java com/actionbarsherlock/widget/ActivityChooserModel.java com/asksven/android/common/kernelutils/Wakelocks.java com/asksven/android/common/kernelutils/WakeupSources.java com/asksven/betterwifionoff/handlers/ConnectionStatusHandler.java com/asksven/betterwifionoff/SsidWhitelistPreference.java com/asksven/betterwifionoff/utils/AppUtil.java com/asksven/android/common/utils/DataStorage.java com/asksven/android/common/kernelutils/State.java com/asksven/android/common/privateapiproxies/KernelWakelock.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				proxies/KernelWakelock.java com/asksven/betterwifionoff/services/EventWatcherService.java com/asksven/betterwifionoff/handlers/ScreenEventHandler.java com/asksven/android/common/kernelutils/NativeKernelWakelock.java com/asksven/betterwifionoff/MainActivity.java com/asksven/android/common/privateapiproxies/NetworkQueryProxy.java com/asksven/betterwifionoff/data/EventDBHelper.java com/asksven/betterwifionoff/services/SetWifiStateService.java com/asksven/betterwifionoff/utils/CellUtil.java com/asksven/betterwifionoff/TimedCheckAlarmReceiver.java com/asksven/android/common/location/GeoUtils.java com/asksven/android/common/privateapiproxies/Process.java com/asksven/betterwifionoff/data/CellDBHelper.java com/asksven/betterwifionoff/WifiLock.java com/asksven/andoid/common/contrib/Debug.java com/asksven/android/common/kernelutils/AlarmsDumpsys.java com/asksven/android/common/wifi/WifiManagerProxy.java
2	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/asksven/android/common/utils/StringUtils.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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/actionbarsherlock/internal/view/menu/MenuBuilder.java
4	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/asksven/betterwifionoff/data/AppWhitelistDBHelper.java com/asksven/betterwifionoff/data/EventDBHelper.java com/asksven/betterwifionoff/data/CellDBHelper.java
5	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/asksven/android/common/utils/DataStorage.java com/asksven/betterwifionoff/MainActivity.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 use no 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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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', 'location'].
5	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to ['system logs'].
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 does not encrypt files 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.
10	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
clients3.google.com	ok	**IP:** 142.251.39.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **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
twitter.com	ok	**IP:** 104.244.42.129 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.773968 **Longitude:** -122.410446 **View:** Google Map

TRACKERS

TRACKER	CATEGORIES	URL
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312

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.