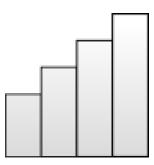


ANDROID STATIC ANALYSIS REPORT



Open WiFi Cleaner(@string/version)

File Name:	installer93.apk
Package Name:	com.dje.openwifinetworkremover
Scan Date:	May 31, 2022, 11:05 a.m.
App Security Score:	53/100 (MEDIUM RISK)
Grade:	

FINDINGS SEVERITY

兼 HIGH	▲ MEDIUM	i INFO	✓ SECURE	्र HOTSPOT
1	4	1	1	0

FILE INFORMATION

File Name: installer93.apk

Size: 0.6MB

MD5: 95264735065f44414b3f46b2c9fd2b7f

SHA1: 7ca01d3a9ccb8787f59bffe11f2978f44acbb39f

SHA256: 38fc429838d0e53ed5f152ec25ad1eaaf015ad776dec5b5d75ac97065057bce5

i APP INFORMATION

App Name: Open WiFi Cleaner

Package Name: com.dje.openwifinetworkremover

 $\textbf{\textit{Main Activity}}: com.dje.open wifine two rkremover. Main Activity$

Target SDK: 19 Min SDK: 8 Max SDK:

Android Version Name: @string/version

Android Version Code: 22

EE APP COMPONENTS

Activities: 2 Services: 0 Receivers: 1 Providers: 0

Exported Activities: O Exported Services: O Exported Receivers: 1 Exported Providers: O

***** 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: 2013-12-15 10:45:09+00:00 Valid To: 2041-05-02 10:45:09+00:00

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

Serial Number: 0x65f9aef3 Hash Algorithm: sha256

md5: 9974b13639d644f41a676c08a2be7d8c

sha1: 577a98a663ed17407c233d28c7bad6db6a2b1769

sha256: 6b985c28fc113386ee4acab5dde71ebf0c9fe94dc867217a90cebdca4ab4ee20

sha512: 3b5600b7d8458a45d2c170e219500ba8596550de45514cc99857bcd32cafacc3b320819dcc2c49f25a7fcdf2dcc44db13e62fd43fa4d46dc59edfe6b796f07ae

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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.

命 APKID ANALYSIS

FILE DETAILS

FILE	DETAILS		
	FINDINGS	DETAILS	
	Compiler	dx (possible dexmerge)	
classes.dex	Manipulator Found	dexmerge	

△ NETWORK SECURITY

	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.

NO	ISSUE	SEVERITY	DESCRIPTION
2	Broadcast Receiver (com.dje.openwifinetworkremover.WifiConnectionHandler) 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
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	com/dje/goodies/debugging/Debug.j ava
2	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/dje/goodies/debugging/Debug.j ava

■ 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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION	
3	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['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 no 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.	

Q DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION

DOMAIN	STATUS	GEOLOCATION	
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	
gnu.org	ok	IP: 209.51.188.116 Country: United States of America Region: Massachusetts City: Boston Latitude: 42.358429 Longitude: -71.059769 View: Google Map	



POSSIBLE SECRETS

"settings_key": "com.dje.openwifinetworkremover.settings"

 $"settings_backup_key": "settings"$

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.