

ANDROID STATIC ANALYSIS REPORT



Dialer for Pebble (3.0)

File Name:	installer100.apk		
Package Name:	com.matejdro.pebbledialer		
Scan Date:	May 31, 2022, 9:47 a.m.		
App Security Score:	46/100 (MEDIUM RISK)		
Grade:			

FINDINGS SEVERITY

派 HIGH	▲ MEDIUM	i INFO	✓ SECURE	[®] HOTSPOT
4	13	1	2	1

FILE INFORMATION

File Name: installer100.apk

Size: 2.26MB

MD5: d4e604263bf500fb9f18a43322378ddd

SHA1: b2370415e81b2ce1ecb81e84bc9ae318038cfc68

SHA256: bed159d5f82166ce12c6411706a272cecc60e2cf81be5e5be5663609e74b1de3

i APP INFORMATION

App Name: Dialer for Pebble

Package Name: com.matejdro.pebbledialer

Main Activity: com.matejdro.pebbledialer.ui.MainActivity

Target SDK: 23 Min SDK: 14 Max SDK:

Android Version Name: 3.0
Android Version Code: 37

B APP COMPONENTS

Activities: 2 Services: 2 Receivers: 7 Providers: 0

Exported Activities: 1 Exported Services: 1 Exported Receivers: 7 Exported Providers: 0



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: 2015-10-15 09:54:03+00:00 Valid To: 2043-03-02 09:54:03+00:00

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

Serial Number: 0x2b6739f1 Hash Algorithm: sha256

md5: 737222ed0195bc6aa3608488412d66e5

sha1: 44a330f17396013d04a526c5c47808a55b7b2d5e

sha256: 51bd25168ef4d200fd4dfd488a582934fe3c41d855475d2512755d6989ef6bcb

sha512: 58f04fc3f6fa298d86fd7efc95a119de7079f7abd330e3fc5a535e3ce011bf90ecbcccd5df0687d1797f16d4b51d681acdd58fd09b988ca5a9a6a05e2b79c3a1

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.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.
android.permission.CALL_PHONE	dangerous	directly call phone numbers	Allows the application to call phone numbers without your intervention. Malicious applications may cause unexpected calls on your phone bill. Note that this does not allow the application to call emergency numbers.
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.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.PROCESS_OUTGOING_CALLS	dangerous	intercept outgoing calls	Allows application to process outgoing calls and change the number to be dialled. Malicious applications may monitor, redirect or prevent outgoing calls.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_SUPERUSER	unknown	Unknown permission	Unknown permission from android reference
android.permission.READ_CALL_LOG	dangerous		Allows an application to read the user's call log.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.SEND_SMS	dangerous	send SMS messages	Allows application to send SMS messages. Malicious applications may cost you money by sending messages without your confirmation.
android.permission.READ_SMS	dangerous	read SMS or MMS	Allows application to read SMS messages stored on your phone or SIM card. Malicious applications may read your confidential messages.
android.permission.WRITE_SMS	dangerous	edit SMS or MMS	Allows application to write to SMS messages stored on your phone or SIM card. Malicious applications may delete your messages.



FILE	DETAILS			
	FINDINGS	DETAILS		
	Anti-VM Code	Build.TAGS check		
classes.dex	Compiler	dx (possible dexmerge)		
	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.matejdro.pebbledialer.CallStatusReceiver) 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.
3	Service (com.matejdro.pebbledialer.notifications.JellybeanNotificationListener) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_NOTIFICATION_LISTENER_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
4	Activity (com.matejdro.pebbledialer.tasker.TaskerSettingsActivity) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
5	Broadcast Receiver (com.matejdro.pebbledialer.pebble.WatchappHandler) 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.
6	Broadcast Receiver (com.matejdro.pebbledialer.tasker.TaskerReceiver) 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 (com.matejdro.pebblecommons.pebble.DataReceiver) 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 (com.matejdro.pebblecommons.messages.TimeVoiceProvider\$VoiceNotificationRemoverReceiver) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
9	Broadcast Receiver (com.matejdro.pebblecommons.userprompt.NativePebbleUserPrompter\$NotificationRemoverReceiver) 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.
10	Broadcast Receiver (com.matejdro.pebblecommons.util.BluetoothHeadsetListener) 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	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	com/matejdro/pebblecommons/util/ RootUtil.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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	timber/log/Timber.java com/matejdro/pebblecommons/util/ ContactUtils.java ar/com/hjg/pngj/PngHelperInternal.ja va ar/com/hjg/pngj/ProgressiveOutputSt ream.java org/java_websocket/WebSocketImpl.j ava com/matejdro/pebbledialer/ui/MainA ctivity.java com/getpebble/android/kit/PebbleKit. java org/java_websocket/server/WebSocke tServer.java com/matejdro/pebblecommons/util/ RTLUtility.java com/matejdro/pebblecommons/vibra tion/VibrationPatternPicker.java
3	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	org/java_websocket/drafts/Draft_75.j ava org/java_websocket/drafts/Draft_76.j ava org/java_websocket/drafts/Draft_10.j ava
4	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	org/java_websocket/drafts/Draft_76.j ava

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	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/matejdro/pebblecommons/util/ AccountRetreiver.java
6	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/getpebble/android/kit/util/Pebbl eDictionary.java
7	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/matejdro/pebblecommons/util/L ogWriter.java
8	SHA-1 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	org/java_websocket/drafts/Draft_10.j ava

■ 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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
2	FCS_STO_EXT.1.1	Security Functional Requirements	Storage of Credentials	The application does not store any credentials to non-volatile memory.
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', 'bluetooth', 'microphone'].
5	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to ['call lists', 'address book'].
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 implement functionality to encrypt sensitive data 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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
11	FCS_HTTPS_EXT.1.3	Selection-Based Security Functional Requirements	HTTPS Protocol	The application notify the user and not establish the connection or request application authorization to establish the connection if the peer certificate is deemed invalid.

Q DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
docs.google.com	ok	IP: 216.58.208.110 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
creativecommons.org	ok	IP: 104.20.151.16 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map

DOMAIN	STATUS	GEOLOCATION
www.paypal.com	ok	IP: 151.101.129.21 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
psdev.de	ok	IP: 49.12.32.214 Country: Germany Region: Sachsen City: Falkenstein Latitude: 50.477879 Longitude: 12.371290 View: Google Map
opensource.org	ok	IP: 172.67.197.41 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
xmlpull.org	ok	IP: 74.50.61.58 Country: United States of America Region: Texas City: Dallas Latitude: 32.814899 Longitude: -96.879204 View: Google Map

DOMAIN	STATUS	GEOLOCATION
www.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
www.apache.org	ok	IP: 151.101.2.132 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
pebble.rickyayoub.com	ok	IP: 192.30.252.153 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
dl.dropboxusercontent.com	ok	IP: 162.125.65.15 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
dev-portal.getpebble.com	ok	No Geolocation information available.

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.