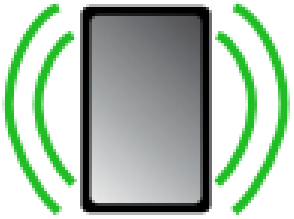
MOBSF

ANDROID STATIC ANALYSIS REPORT



RingyDingyDingy (0.7.5)

File Name:	installer247.apk
Package Name:	com.dririan.RingyDingyDingy
Scan Date:	May 31, 2022, 12:22 p.m.
App Security Score:	39/100 (HIGH RISK)
Grade:	C

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
4	7	1	1	1

FILE INFORMATION

File Name: installer247.apk
Size: 0.08MB
MD5: d068937c3c4490ca4cae1a25e3d53133
SHA1: 8410b7fbba7877021aa4b39d6690fecac9ca7b30
SHA256: b184b9e82a5914f2bb79e851a3c08ee89b8247e17d92c1b9a79f07b34bf14d15

APP INFORMATION

App Name: RingyDingyDingy
Package Name: com.dririan.RingyDingyDingy
Main Activity: .MainActivity
Target SDK: 17
Min SDK: 4
Max SDK:
Android Version Name: 0.7.5
Android Version Code: 705

APP COMPONENTS

Activities: 4
Services: 0
Receivers: 8
Providers: 0
Exported Activities: 0
Exported Services: 0
Exported Receivers: 4
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: 2012-08-10 08:56:43+00:00
Valid To: 2039-12-27 08:56:43+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x5024cccb
Hash Algorithm: sha1
md5: f68cccda970bb7eb1c09b832d1db48a1
sha1: 6456b31e70a0554187c975ffa77c0058bfcd39c4
sha256: 67f1c0d6aa6d2485a471534afd5d6fc7ba06c7ddd3a4601dd8215777a10cd3c9
sha512: 4932c6fdcf52435f6eb90c5c7bfa3bc2c878e8fbab46f154b448b512d563af3dc51999f01db88266f50553fbf9fa60960abce5ce45e268e9dad7761bf7cac924

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.
Certificate algorithm might be vulnerable to hash collision	high	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues.

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.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.RECEIVE_SMS	dangerous	receive SMS	Allows application to receive and process SMS messages. Malicious applications may monitor your messages or delete them without showing them to you.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.apps.googlevoice.permission.RECEIVE_SMS	dangerous	receive SMS	Allows application to receive and process SMS messages. Malicious applications may monitor your messages or delete them without showing them to you.
com.dririan.RingyDingyDingy.EXECUTE_COMMAND	unknown	Unknown permission	Unknown permission from android reference
com.dririan.RingyDingyDingy.HANDLE_COMMAND	unknown	Unknown permission	Unknown permission from android reference
com.dririan.RingyDingyDingy.HANDLE_INTERNAL_COMMAND	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Compiler — DETAILS: dx

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.
2	Broadcast Receiver (.ApiHandler) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.dririan.RingyDingyDingy.EXECUTE_COMMAND protectionLevel: dangerous [android:exported=true]	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. It is protected by a permission. However, the protection level of the permission is set to dangerous. This means that a malicious application can request and obtain the permission and interact with the component. If it was set to signature, only applications signed with the same certificate could obtain the permission.
3	Broadcast Receiver (.GoogleVoiceReceiver) 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.
4	Broadcast Receiver (.LogHandler) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.dririan.RingyDingyDingy.EXECUTE_COMMAND protectionLevel: dangerous [android:exported=true]	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. It is protected by a permission. However, the protection level of the permission is set to dangerous. This means that a malicious application can request and obtain the permission and interact with the component. If it was set to signature, only applications signed with the same certificate could obtain the permission.
5	Broadcast Receiver (.SmsReceiver) 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	High Intent Priority (1000) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.

NO	ISSUE	SEVERITY	DESCRIPTION
7	High Intent Priority (2147483645) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.

</> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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	com/dririan/RingyDingyDingy/PreferencesManager.java
2	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/dririan/RingyDingyDingy/LogDatabase.java com/dririan/RingyDingyDingy/LogOpenHelper.java
3	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/dririan/RingyDingyDingy/SmsErrorHandler.java com/dririan/RingyDingyDingy/RemoteRingActivity.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.
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 no hardware resources.
5	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to ['address book'].
6	FDP_NET_EXT.1.1	Security Functional Requirements	Network Communications	The application has no 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 not encrypt any data in traffic or does not transmit any data between itself and another trusted IT product.

EMAILS

EMAIL	FILE
ringydingydingy@dririan.com	Android String Resource

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.