MOBSF

ANDROID STATIC ANALYSIS REPORT

Inetify (2.1.2)

File Name:	installer78.apk
Package Name:	net.luniks.android.inetify
Scan Date:	May 31, 2022, 11:10 a.m.
App Security Score:	47/100 (MEDIUM RISK)
Grade:	

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	7	1	1	1

FILE INFORMATION

File Name: installer78.apk
Size: 0.41MB
MD5: 40a719422d9f7a9543d161ede1ffc531
SHA1: 71915b1c10ce6a9d23a5692204294d903dbd1e26
SHA256: d09d8cfefe9efc3c468c2ce2dd28e6ed8c9dd98d27d9cfe39c501ff6f84cdab7

APP INFORMATION

App Name: Inetify
Package Name: net.luniks.android.inetify
Main Activity: .Inetify
Target SDK: 10
Min SDK: 7
Max SDK:
Android Version Name: 2.1.2
Android Version Code: 20

APP COMPONENTS

Activities: 7
Services: 2
Receivers: 3
Providers: 0
Exported Activities: 0
Exported Services: 0
Exported Receivers: 2
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: 2012-09-04 16:30:37+00:00
Valid To: 2040-01-21 16:30:37+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x50462cad
Hash Algorithm: sha1
md5: 3ac7523b75f36764ff6959603c5f1e87
sha1: c36a021ca1350eb40f4f08cddf2c9c9cee0b98fc
sha256: 55604cad67e25df74518650a4ab474246a4150767ba00f38a9c29f1e2b05d0de
sha512: 802bb854206dcc40815e1cb577867aaf84844a065c2b84ffcd76008de3b79fc868aaa360eda8380832a3438960e0aff3715adc3c4d1e923df15fc3b98ddf7a79

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.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.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.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.

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.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.ACCESS_MOCK_LOCATION	dangerous	mock location sources for testing	Create mock location sources for testing. Malicious applications can use this to override the location and/or status returned by real-location sources such as GPS or Network providers.

APKID ANALYSIS

FILE	DETAILS

FILE	DETAILS
classes.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check</td></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] 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.
2	Broadcast Receiver (.ConnectivityActionReceiver) 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
3	Broadcast Receiver (.LocationAlarmControllerReceiver) 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	org/slf4j/helpers/MessageFormatter.java org/slf4j/helpers/Util.java org/slf4j/impl/AndroidLogger.java org/jsoup/examples/ListLinks.java org/metalev/multitouch/controller/MultiTouchController.java
2	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	org/osmdroid/contributor/util/constants/OpenStreetMapContributorConstants.java org/jsoup/nodes/XmlDeclaration.java org/osmdroid/tileprovider/util/CloudmadeUtil.java org/jsoup/nodes/DataNode.java org/jsoup/nodes/TextNode.java org/jsoup/nodes/Comment.java org/osmdroid/tileprovider/modules/DatabaseFileArchive.java
3	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	org/osmdroid/tileprovider/constants/OpenStreetMapTileProviderConstants.java org/osmdroid/tileprovider/modules/MapTileFileStorageProviderBase.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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	net/luniks/android/inetify/DatabaseAdapterImpl.java
5	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/osmdroid/tileprovider/tilesource/BitmapTileSourceBase.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 ['network connectivity', 'location'].
5	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
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 not encrypt any data in traffic or does not transmit any data between itself and another trusted IT product.

🔍 DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
otile2.mqcdn.com	ok	No Geolocation information available.
b.tile.openstreetmap.org	ok	**IP:** 151.101.38.137 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
b.tile.opencyclemap.org	ok	**IP:** 136.243.152.14 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
a.tile.openstreetmap.org	ok	**IP:** 151.101.38.137 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
auth.cloudmade.com	ok	**IP:** 23.21.136.107 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
www.slf4j.org	ok	**IP:** 83.173.251.158 **Country:** Switzerland **Region:** Zurich **City:** Zurich **Latitude:** 47.366669 **Longitude:** 8.550000 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
overlay.openstreetmap.nl	ok	**IP:** 93.186.176.173 **Country:** Netherlands **Region:** Overijssel **City:** Enschede **Latitude:** 52.218330 **Longitude:** 6.895830 **View:** Google Map
code.google.com	ok	**IP:** 142.250.179.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
api.tiles.mapbox.com	ok	**IP:** 18.65.34.184 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
c.tile.opencyclemap.org	ok	**IP:** 136.243.152.14 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.openstreetmap.org	ok	**IP:** 130.117.76.12 **Country:** United States of America **Region:** Georgia **City:** Atlanta **Latitude:** 33.749001 **Longitude:** -84.387978 **View:** Google Map
www.w3.org	ok	**IP:** 128.30.52.100 **Country:** United States of America **Region:** Massachusetts **City:** Cambridge **Latitude:** 42.365078 **Longitude:** -71.104523 **View:** Google Map
b.tile.cloudmade.com	ok	No Geolocation information available.
www.google.de	ok	**IP:** 142.250.179.195 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
otile4.mqcdn.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.oxygen-icons.org	ok	**IP:** 92.205.3.60 **Country:** Germany **Region:** Nordrhein-Westfalen **City:** Koeln **Latitude:** 50.933331 **Longitude:** 6.950000 **View:** Google Map
jsoup.org	ok	**IP:** 188.114.97.0 **Country:** Spain **Region:** Madrid, Comunidad de **City:** Madrid **Latitude:** 40.416500 **Longitude:** -3.702560 **View:** Google Map
a.tile.cloudmade.com	ok	No Geolocation information available.
www.google.com	ok	**IP:** 142.250.179.164 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
otile3.mqcdn.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
c.tile.openstreetmap.org	ok	**IP:** 151.101.38.137 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
topo.geofabrik.de	ok	No Geolocation information available.
topo.openstreetmap.de	ok	No Geolocation information available.
otile1.mqcdn.com	ok	No Geolocation information available.
www.placeyourdomainhere.com	ok	**IP:** 54.249.56.71 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** Google Map
openptmap.org	ok	**IP:** 88.99.141.112 **Country:** Germany **Region:** Sachsen **City:** Falkenstein **Latitude:** 50.477879 **Longitude:** 12.371290 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
a.tile.opencyclemap.org	ok	**IP:** 88.99.98.237 **Country:** Germany **Region:** Bayern **City:** Gunzenhausen **Latitude:** 48.323330 **Longitude:** 11.601220 **View:** Google Map
c.tile.cloudmade.com	ok	No Geolocation information available.
www.andnav.org	ok	**IP:** 188.114.96.0 **Country:** Spain **Region:** Madrid, Comunidad de **City:** Madrid **Latitude:** 40.416500 **Longitude:** -3.702560 **View:** Google Map
www.topografix.com	ok	**IP:** 104.209.197.87 **Country:** United States of America **Region:** Virginia **City:** Boydton **Latitude:** 36.667641 **Longitude:** -78.387497 **View:** Google Map

EMAILS

EMAIL	FILE
gmdode@gmail.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.