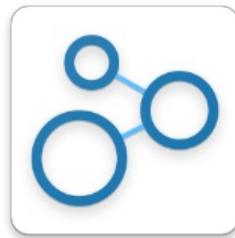




ANDROID STATIC ANALYSIS REPORT



 DAPNET (1.0.16)

File Name:

installer341.apk

Package Name:

de.hampager.dapnetmobile

Scan Date:

May 31, 2022, 4:14 p.m.






App Security Score:

60/100 (LOW RISK)

Grade:



FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
1	6	1	2	1

FILE INFORMATION

File Name: installer341.apk

Size: 2.98MB

MD5: edaf55605ee6166cf54cfe30ca734c0c

SHA1: e9929c0948199fe2b0ee12f1729c7ec445920858

SHA256: 4b465ffc74c6c07449e952779391b60d4dd9932196e43c72a93d6bec92bd809f

APP INFORMATION

App Name: DAPNET

Package Name: de.hampager.dapnetmobile

Main Activity: de.hampager.dapnetmobile.MainActivity

Target SDK: 25

Min SDK: 15

Max SDK:

Android Version Name: 1.0.16

Android Version Code: 21

APP COMPONENTS

Activities: 3

Services: 0

Receivers: 0

Providers: 0

Exported Activities: 1

Exported Services: 0

Exported Receivers: 0

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: 2017-05-20 22:01:23+00:00

Valid To: 2044-10-05 22:01:23+00:00

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

Serial Number: 0x135d6f20

Hash Algorithm: sha256

md5: cc9fd4b5988bcf17bb2cfee05dbf4840

sha1: 3fe4d609790620596fdb23ac5b0ba28aed874166

sha256: f3bd72be60bd04aea13cc94a499ce7d4e67a0138aaa74f1c152088a7d872a4d1

sha512: fbf5007efccf3daeee07a15e9537156b52d44d99330c4768f0b14ba2806fecafad382e941f6e9467398462b16a3c15cd9b8f52294e8e8b8dd9c8a0adf25017d7

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.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.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.

APKID ANALYSIS

FILE	DETAILS
------	---------

FILE	DETAILS	
classes.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.MANUFACTURER check
	Compiler	r8 without marker (suspicious)

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	Activity (de.hampager.dapnetmobile.LoginActivity) 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.

CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
				org/osmdroid/views/overlay/DefaultOverlayManager.java org/osmdroid/tileprovider/util/CloudmadeUtil.java org/osmdroid/views/MapView.java org/osmdroid/tileprovider/modules/ZipFileArchive.java org/osmdroid/tileprovider/modules/MapTileModuleProviderBase.java org/osmdroid/tileprovider/modules/SqlTileWriter.java org/osmdroid/tileprovider/modules/MapTileFileArchiveProvider.java org/osmdroid/events/DelayedMapListener.java com/tokenautocomplete/TokenCompleteTextView.java org/osmdroid/tileprovider/modules/MapTileFileStorageProviderBase.java de/hampager/dapnetmobile/MainActivity.java org/osmdroid/tileprovider/modules/MapTileDownloader.java de/hampager/dapnetmobile/fragments/MapFragment.java org/osmdroid/views/overlay/gridlines/LatLonGridlineOverlay.java org/osmdroid/tileprovider/modules/MapTileFilesystemProvider.java de/hampager/dapnetmobile/fragments/WelcomeFragment.java org/osmdroid/tileprovider/cachemanager/CacheManager.java org/osmdroid/tileprovider/util/StorageUtils.java org/osmdroid/views/overlay/NonAcceleratedOverlay.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	org/osmdroid/tileprovider/modules/G FileArchive.java org/metalev/multitouch/controller/Mul tiTouchController.java de/hampager/dapnetmobile/PostCallA ctivity.java de/hampager/dapnetmobile/LoginActi vity.java org/osmdroid/tileprovider/tilesources/C loudmadeTileSource.java org/osmdroid/views/overlay/infowind ow/InfoWindow.java org/osmdroid/tileprovider/util/Manifes tUtil.java org/osmdroid/tileprovider/LRUMapTile Cache.java org/osmdroid/tileprovider/modules/D atabaseFileArchive.java org/osmdroid/tileprovider/MapTilePro viderBase.java org/osmdroid/tileprovider/util/Counter s.java org/osmdroid/tileprovider/MapTileCac he.java org/osmdroid/tileprovider/tilesources/B itmapTileSourceBase.java org/osmdroid/views/overlay/infowind ow/MarkerInfoWindow.java org/osmdroid/tileprovider/tilesources/b ing/BingMapTileSource.java org/osmdroid/tileprovider/modules/Of flineTileProvider.java org/osmdroid/views/overlay/mylocatio n/GpsMyLocationProvider.java de/hampager/dapnetmobile/fragments /CallFragment.java org/osmdroid/tileprovider/modules/Ar chiveFileFactory.java org/osmdroid/tileprovider/modules/M BTilesFileArchive.java org/osmdroid/views/overlay/TilesOverl

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ay.java org/osmdroid/tileprovider/modules/TileWriter.java
				org/osmdroid/views/overlay/mylocation/MyLocationNewOverlay.java de/hampager/dapnetmobile/adapters/CallAdapter.java org/osmdroid/tileprovider/MapTileProviderArray.java org/osmdroid/tileprovider/modules/SQLiteArchiveTileWriter.java org/osmdroid/tileprovider/modules/MapTileSqlCacheProvider.java org/osmdroid/config/DefaultConfigurationProvider.java org/osmdroid/views/overlay/infowindow/BasicInfoWindow.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/tileprovider/util/CloudmadeUtil.java org/osmdroid/tileprovider/modules/SQLiteTileWriter.java org/osmdroid/tileprovider/modules/DatabaseFileArchive.java org/osmdroid/tileprovider/tilesources/bing/BingMapTileSource.java
3	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	org/osmdroid/tileprovider/modules/SQLiteTileWriter.java org/osmdroid/tileprovider/modules/DatabaseFileArchive.java org/osmdroid/tileprovider/modules/SQLiteArchiveTileWriter.java
4	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/modules/MapTileFileStorageProviderBase.java org/osmdroid/tileprovider/util/StorageUtils.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	de/hampager/dapnetmobile/api/ServiceGenerator.java
6	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/tilesources/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'].
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 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.
11	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.
12	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.
13	FIA_X509_EXT.2.1	Selection-Based Security Functional Requirements	X.509 Certificate Authentication	The application use X.509v3 certificates as defined by RFC 5280 to support authentication for HTTPS , TLS.

DOMAIN	STATUS	GEOLOCATION
b.tile.thunderforest.com	ok	IP: 136.243.152.14 Country: Germany Region: Hessen City: Frankfurt am Main Latitude: 50.115520 Longitude: 8.684170 View: Google Map
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
c.tiles.wmflabs.org	ok	IP: 185.15.56.55 Country: United States of America Region: California City: San Francisco Latitude: 37.788464 Longitude: -122.394608 View: Google Map
wms.chartbundle.com	ok	IP: 138.68.60.210 Country: United States of America Region: California City: Santa Clara Latitude: 37.354111 Longitude: -121.955238 View: Google Map

DOMAIN	STATUS	GEOLOCATION
opentopomap.org	ok	IP: 131.188.76.144 Country: Germany Region: Bayern City: Erlangen Latitude: 49.595612 Longitude: 10.994970 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
a.tile.thunderforest.com	ok	IP: 88.99.99.5 Country: Germany Region: Sachsen City: Falkenstein Latitude: 50.477879 Longitude: 12.371290 View: Google Map
1.domain	ok	No Geolocation information available.
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

DOMAIN	STATUS	GEOLOCATION
3.domain	ok	No Geolocation information available.
www.afu.rwth-aachen.de	ok	IP: 137.226.79.98 Country: Germany Region: Nordrhein-Westfalen City: Aachen Latitude: 50.776642 Longitude: 6.083420 View: Google Map
overlay.openstreetmap.nl	ok	IP: 93.186.176.173 Country: Netherlands Region: Overijssel City: Enschede Latitude: 52.218330 Longitude: 6.895830 View: Google Map
dapnet.db0sda.ampr.org	ok	IP: 44.149.166.27 Country: United States of America Region: California City: San Diego Latitude: 32.800457 Longitude: -117.171066 View: Google Map
hampager.de	ok	IP: 137.226.79.98 Country: Germany Region: Nordrhein-Westfalen City: Aachen Latitude: 50.776642 Longitude: 6.083420 View: Google Map

DOMAIN	STATUS	GEOLOCATION
www.hampager.de	ok	IP: 137.226.79.98 Country: Germany Region: Nordrhein-Westfalen City: Aachen Latitude: 50.776642 Longitude: 6.083420 View: Google Map
tiles.openseamap.org	ok	IP: 195.37.132.70 Country: Germany Region: Rheinland-Pfalz City: Franken Latitude: 50.501240 Longitude: 7.234600 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
db0sda.ampr.org	ok	IP: 44.149.166.2 Country: United States of America Region: California City: San Diego Latitude: 32.800457 Longitude: -117.171066 View: Google Map
b.tile.cloudmade.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
2.domain	ok	No Geolocation information available.
basemap.nationalmap.gov	ok	IP: 108.156.60.29 Country: United States of America Region: Washington City: Redmond Latitude: 47.682899 Longitude: -122.120903 View: Google Map
c.tile.thunderforest.com	ok	IP: 88.99.98.237 Country: Germany Region: Bayern City: Gunzenhausen Latitude: 48.323330 Longitude: 11.601220 View: Google Map
a.tile.cloudmade.com	ok	No Geolocation information available.
a.tiles.wmflabs.org	ok	IP: 185.15.56.55 Country: United States of America Region: California City: San Francisco Latitude: 37.788464 Longitude: -122.394608 View: Google Map

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
dev.virtualearth.net	ok	IP: 52.156.193.145 Country: Ireland Region: Dublin City: Dublin Latitude: 53.343990 Longitude: -6.267190 View: Google Map
b.tiles.wmflabs.org	ok	IP: 185.15.56.55 Country: United States of America Region: California City: San Francisco Latitude: 37.788464 Longitude: -122.394608 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
c.tile.cloudmade.com	ok	No Geolocation information available.

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
4.domain	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](#).