



ANDROID STATIC ANALYSIS REPORT



 AsteroidOS Sync (0.16)

File Name:

installer130.apk

Package Name:

org.asteroidos.sync

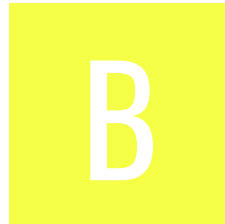
Scan Date:






May 31, 2022, 11:52 a.m.

App Security Score:

58/100 (MEDIUM RISK)

Grade:



 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
1	8	1	2	1

FILE INFORMATION

File Name: installer130.apk

Size: 3.4MB

MD5: 1fe06e161c4b03093b160f8c7e5390f6

SHA1: 0d19fcb8cb92ff2b7c61678976ee20b9dc60ea50

SHA256: 8e89725c847068991c224fedde0f1da68f43d68e7a8705aa881fb50a16d833aa

APP INFORMATION

App Name: AsteroidOS Sync

Package Name: org.asteroidos.sync

Main Activity: org.asteroidos.sync.PermissionsActivity

Target SDK: 29

Min SDK: 21

Max SDK:

Android Version Name: 0.16

Android Version Code: 16

APP COMPONENTS

Activities: 2

Services: 2

Receivers: 1

Providers: 1

Exported Activities: 0

Exported Services: 1
Exported Receivers: 1
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: 2016-12-09 00:03:58+00:00
Valid To: 2044-04-26 00:03:58+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x42e72044
Hash Algorithm: sha256
md5: cc002549aee812aa262365248d9b137c
sha1: 937a4f44aea0316b296f1f4d2a571751a81d0a48
sha256: 6366670ec625122d29b05c9710bfae491f975b232071803b36768cac76d065a5
sha512: fee40adc53068ce7400e55095701420ba854650faf55ee69c1c3a9c778375e34236cf064cbd497acd6a1cf5ea41ff5ea28df92dfd6a91d2d2c61d194e7802885

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
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
------------	--------	------	-------------

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.
android.permission.BLUETOOTH_PRIVILEGED	SignatureOrSystem		Allows applications to pair bluetooth devices without user interaction, and to allow or disallow phonebook access or message access. This is not available to third party applications.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_LOCATION	unknown	Unknown permission	Unknown permission from android reference
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.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.

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.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground.
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	normal		Permission an application must hold in order to use Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.

APKID ANALYSIS

FILE	DETAILS	
classes.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.MANUFACTURER check
	Compiler	r8

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
org.asteroidos.sync.PermissionsActivity	Schemes: http://, Hosts: sync.asteroidos.org, Path Prefixes: /,

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	Service (org.asteroidos.sync.services.NLService) 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.
3	Broadcast Receiver (org.asteroidos.sync.services.AutostartService) 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
				org/osmdroid/tileprovider/util/Counters.java org/metalev/multitouch/controller/MultiTouchController.java org/osmdroid/views/overlay/TilesOverlay.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				org/osmdroid/views/overlay/InfoWindow.java org/osmdroid/views/overlay/infowindow/InfoWindow.java org/asteroidos/sync/ble/MediaService.java org/osmdroid/tileprovider/modules/DatabaseFileArchive.java org/osmdroid/tileprovider/modules/SQLiteArchiveTileWriter.java org/osmdroid/views/overlay/DefaultOverlayManager.java org/osmdroid/events/DelayedMapListener.java org/osmdroid/tileprovider/BitmapPool.java org/osmdroid/tileprovider/modules/OfflineTileProvider.java org/asteroidos/sync/ble/WeatherService.java org/asteroidos/sync/ble/NotificationService.java org/osmdroid/views/MapView.java org/osmdroid/tileprovider/modules/MapTileSqlCacheProvider.java com/idevicesinc/sweetblue/P_BluetoothCrashResolver.java org/asteroidos/sync/ble/ScreenshotService.java org/osmdroid/tileprovider/modules/MapTileFilesystemProvider.java org/osmdroid/tileprovider/modules/GEMFFileArchive.java org/asteroidos/sync/utils/AppInfoHelper.java com/idevicesinc/sweetblue/backend/historical/Backend_HistoricalDataList_Default.java com/idevicesinc/sweetblue/WriteBuilder.java org/osmdroid/tileprovider/util/StorageUtils.java org/osmdroid/views/overlay/gridlines/LatLonGridlineOverlay.java org/osmdroid/views/overlay/infowindow/BasicInfoWindow.java org/osmdroid/views/overlay/NonAcceleratedOverlay.java org/osmdroid/tileprovider/modules/ArchiveFileFactory.java org/osmdroid/tileprovider/modules/TileWriter.java org/osmdroid/tileprovider/modules/MapTileModuleProviderBase.java org/osmdroid/tileprovider/modules/SqlTileWriter.java

NO	The App logs information. Sensitive information should never be logged.	SEVERITY INFO	CWE: CWE-532: Insertion of Sensitive Information into Log File STANDARDS OWASP MASVS: MSTG-STORAGE-3	FILES
				org/osmdroid/tileprovider/modules/MapTileFileArchiveProvider.java org/osmdroid/tileprovider/tilesource/bing/BingMapTileSource.java com/idevicesinc/sweetblue/BleManager.java org/osmdroid/tileprovider/util/ManifestUtil.java com/idevicesinc/sweetblue/P_WakeLockManager.java org/osmdroid/tileprovider/tilesource/BitmapTileSourceBase.java org/osmdroid/tileprovider/MapTileProviderBase.java org/osmdroid/tileprovider/MapTileCache.java org/osmdroid/tileprovider/util/CloudmadeUtil.java org/osmdroid/tileprovider/modules/ZipFileArchive.java org/osmdroid/tileprovider/modules/TileDownloader.java org/osmdroid/views/overlay/mylocation/MyLocationNewOverlay.java com/idevicesinc/sweetblue/Utils/Utils_Reflection.java org/osmdroid/tileprovider/cachemanager/CacheManager.java org/osmdroid/config/DefaultConfigurationProvider.java com/idevicesinc/sweetblue/compat/L_Util.java org/osmdroid/views/overlay/infowindow/MarkerInfoWindow.java org/osmdroid/tileprovider/tilesource/CloudmadeTileSource.java org/osmdroid/tileprovider/modules/MBTilesFileArchive.java com/maxmpz/poweramp/player/PowerampAPIHelper.java com/idevicesinc/sweetblue/Utils/BluetoothEnabler.java org/asteroidos/sync/adapters/AppInfoAdapter.java com/idevicesinc/sweetblue/Utils/TimeTracker.java io/github/dreierf/materialintroscreen/widgets/CustomViewPager.java

NO	ISSUE	SEVERITY	STANDARDS	org/asteroidos/sync/ble/TimeService.java com/idevicesinc/sweetblue/Utils/Utils_ScanRecord.java
				org/osmdroid/views/overlay/mylocation/GpsMyLocationProvider.java org/osmdroid/tileprovider/modules/MapTileDownloader.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	org/osmdroid/tileprovider/modules/DatabaseFileArchive.java org/osmdroid/tileprovider/modules/SqliteArchiveTileWriter.java org/osmdroid/tileprovider/modules/SqlTileWriter.java
3	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/modules/DatabaseFileArchive.java org/asteroidos/sync/ble/WeatherService.java org/osmdroid/tileprovider/modules/SqlTileWriter.java org/osmdroid/tileprovider/tilesource/bing/BingMapTileSource.java com/idevicesinc/sweetblue/BleManager.java org/osmdroid/tileprovider/util/CloudmadeUtil.java com/idevicesinc/sweetblue/P_UhOhThrottler.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/asteroidos/sync/ble/ScreenshotService.java org/osmdroid/tileprovider/util/StorageUtils.java
5	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	okio/Buffer.java
6	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	github/vatsal/easyweather/retrofit/api/ApiClient.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	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', 'bluetooth', 'location'].
5	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to no sensitive information repositories.
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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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 MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
developer.android.com	ok	IP: 142.250.179.206 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

DOMAIN	STATUS	GEOLOCATION
b.tile.thunderforest.com	ok	IP: 88.99.70.11 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
api.openweathermap.org	ok	IP: 82.196.7.246 Country: Netherlands Region: Noord-Holland City: Amsterdam Latitude: 52.374031 Longitude: 4.889690 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: 88.99.98.237 Country: Germany Region: Bayern City: Gunzenhausen Latitude: 48.323330 Longitude: 11.601220 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
3.domain	ok	No Geolocation information available.

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
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
openweathermap.org	ok	IP: 138.201.197.100 Country: Germany Region: Hessen City: Frankfurt am Main Latitude: 50.115520 Longitude: 8.684170 View: Google Map
tiles.openseamap.org	ok	No Geolocation information available.
c.tile.opentopomap.org	ok	IP: 131.188.76.144 Country: Germany Region: Bayern City: Erlangen Latitude: 49.595612 Longitude: 10.994970 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: 65.9.85.6 Country: United States of America Region: Washington City: Seattle Latitude: 47.606209 Longitude: -122.332069 View: Google Map
c.tile.thunderforest.com	ok	IP: 88.99.99.5 Country: Germany Region: Sachsen City: Falkenstein Latitude: 50.477879 Longitude: 12.371290 View: Google Map
a.tile.cloudmade.com	ok	No Geolocation information available.
api.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
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

DOMAIN	STATUS	GEOLOCATION
b.tile.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.opentopomap.org	ok	IP: 131.188.76.144 Country: Germany Region: Bayern City: Erlangen Latitude: 49.595612 Longitude: 10.994970 View: Google Map
c.tile.cloudmade.com	ok	No Geolocation information available.
4.domain	ok	No Geolocation information available.

EMAILS

EMAIL	FILE
sweetblue@idevicesinc.com	com/idevicesinc/sweetblue/backend/historical/Backend_HistoricalDataList_Default.java

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.