



ANDROID STATIC ANALYSIS REPORT



 Cuberite (1.5.3)

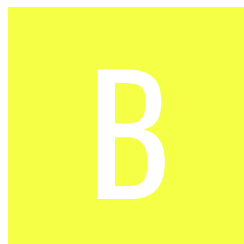
File Name: installer287.apk

Package Name: org.cuberite.android






Scan Date: May 31, 2022, 11:32 a.m.

App Security Score: 46/100 (MEDIUM RISK)

Grade:



FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
2	6	1	1	1

FILE INFORMATION

File Name: installer287.apk

Size: 1.53MB

MD5: 0c5849d0d65b8d18692202ef956cf430

SHA1: 78bceee9b625c900b164e319b184b0ffbaea2317

SHA256: 843407d18efa2463b1ce56038a1830c378dbe042c14a753a17289e37e5b35ad8

APP INFORMATION

App Name: Cuberite

Package Name: org.cuberite.android

Main Activity: org.cuberite.android.MainActivity

Target SDK: 28

Min SDK: 16

Max SDK:

Android Version Name: 1.5.3

Android Version Code: 11

APP COMPONENTS

Activities: 1
Services: 2
Receivers: 1
Providers: 0
Exported Activities: 0
Exported Services: 0
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: 2020-08-08 08:04:49+00:00
Valid To: 2047-12-25 08:04:49+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x5db219d2
Hash Algorithm: sha256
md5: 4d845d049022869562de07974d350f5a
sha1: c43b7bcfd364154e579036d4d86b56606348a918
sha256: 0587d1acc68c8e7f4f63399b1a36d4689f6bb1a8b5c1e90810e75e31c441c8c6
sha512: 30bdbe80fc929656a0c1675427124e9c0f674476dd5d6600eb543de7f6df47086a9a90540889c134da3ec1fef04deaf4e0cc900c584d1f7f274bcfbdb5be39775

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.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
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.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.

APKID ANALYSIS

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

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION
----	-------	----------	-------------

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.

NO	ISSUE	SEVERITY	DESCRIPTION
2	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.
3	Broadcast Receiver (org.cuberite.android.receivers.StartupReceiver) 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
				a/g/l/z.java a/g/f/e.java a/b/l/a/a.java a/b/p/i/d.java a/j/d/q.java a/g/f/g.java a/g/e/b/h.java a/b/q/a0.java c/a/a/b/r.java a/j/d/y.java a/g/l/u.java c/a/a/a.java a/s/a/a/h.java a/g/d/c.java a/j/d/a.java b/b/a/a/f0/b.java a/b/q/d1.java a/g/d/b.java a/b/q/a1.java a/b/k/j.java a/g/f/d/ia

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/n/a.java a/b/g/n0.java a/b/q/m0.java a/b/q/s0.java a/g/l/h.java c/a/a/b/b.java a/j/d/z.java a/j/d/d.java c/a/a/b/o.java a/g/d/g.java b/b/a/a/i0/g.java org/cuberite/android/MainActivity.java b/b/a/a/m/g.java c/a/a/b/h.java a/o/f.java a/g/l/b.java org/cuberite/android/services/CuberiteService.java a/b/k/v.java c/a/a/c/a.java a/h/a/b.java a/b/k/m.java a/r/x.java a/b/q/z0.java b/b/a/a/g0/b.java a/i/b/e.java org/cuberite/android/services/InstallService.java a/g/l/q.java a/g/f/k/d.java c/a/a/b/a.java a/g/h/b.java a/b/q/k0.java a/b/k/l.java a/j/d/o0.java a/r/i0.java a/b/p/i/g.java a/n/a/a.java a/g/f/f.java a/g/j/b.java a/b/p/f.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a/g/r/c.java a/j/d/w.java a/g/l/a.java c/a/a/b/p.java a/g/f/j.java a/j/d/f.java b/b/a/a/d0/b.java a/j/d/s.java a/b/q/w.java a/b/q/r0.java a/b/q/e0.java
2	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/cuberite/android/MainActivity.java c/a/a/b/i.java
3	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	c/a/a/c/a.java
4	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/cuberite/android/services/InstallService.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_STO_EXT.1.1	Security Functional Requirements	Storage of Credentials	The application does not store any credentials to non-volatile memory.
2	FCS_CKM_EXT.1.1	Security Functional Requirements	Cryptographic Key Generation Services	The application generate no asymmetric cryptographic keys.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
3	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['network connectivity'].
4	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to no sensitive information repositories.
5	FDP_NET_EXT.1.1	Security Functional Requirements	Network Communications	The application has user/application initiated network communications.
6	FDP_DAR_EXT.1.1	Security Functional Requirements	Encryption Of Sensitive Application Data	The application does not encrypt files in non-volatile memory.
7	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.
8	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.
9	FCS_COP.1.1(2)	Selection-Based Security Functional Requirements	Cryptographic Operation - Hashing	The application perform cryptographic hashing services in accordance with a specified cryptographic algorithm SHA-1/SHA-256/SHA-384/SHA-512 and message digest sizes 160/256/384/512 bits.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
download.cuberite.org	ok	IP: 91.121.65.133 Country: France Region: Hauts-de-France City: Roubaix Latitude: 50.694210 Longitude: 3.174560 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
schemas.android.com	ok	No Geolocation information available.

HARDCODED SECRETS

POSSIBLE SECRETS
"password" : "Password"
"settings_authentication_toggle" : "Authentication"
"username" : "Username"
"password" : "Passwort"

POSSIBLE SECRETS
"username" : "Benutzername"
"password" : "Wachtwoord"
"settings_authentication_toggle" : "Authenticatie"
"username" : "Gebruikersnaam"
"password" : "Senha"

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](#).