ANDROID STATIC ANALYSIS REPORT

xManager (3.2)

File Name:	xManager.apk
Package Name:	com.xc3fff0e.xmanager
Scan Date:	Jan. 6, 2023, 2:31 a.m.
App Security Score:	45/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	2/428

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	✓ SECURE	HOTSPOT
1	10	2	0	1

FILE INFORMATION

File Name: xManager.apk
Size: 6.01MB
MD5: d052eaa352fee6eccb905609a06b16d3
SHA1: c63ec9710ff8cf3a7aa97f149f11e23d720001d5
SHA256: 81db65f8717adc4e3e983a6e3815d1ca5d541a6a995901ede485662dbeab038b

APP INFORMATION

App Name: xManager
Package Name: com.xc3fff0e.xmanager
Main Activity: .SplashActivity
Target SDK: 31
Min SDK: 21
Max SDK:
Android Version Name: 3.2

Android Version Code: 2

APP COMPONENTS

Activities: 7
Services: 2
Receivers: 1
Providers: 2
Exported Activities: 2
Exported Services: 0
Exported Receivers: 1
Exported Providers: 0

CERTIFICATE INFORMATION

```
APK is signed
v1 signature: True
v2 signature: True
v3 signature: True
Found 1 unique certificates
Subject: CN=xC3FFF0E
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2022-03-07 19:54:28+00:00
Valid To: 2122-05-22 19:54:28+00:00
Issuer: CN=xC3FFF0E
Serial Number: 0x622662f4
Hash Algorithm: sha512
md5: 31bc55e016e22cf70dcb6b914412f0dc
sha1: 2a3a728e9547dc4917ae3c7c31c982fcd3004764
sha256: 3e54b1147dbcc14ca12198d9613f3f2514adc4e8b616a17991c9db0e6ae22158
sha512: 7aa28b11d5ef974152a01437f163265ee8054edf4a68fcb76324fabc20acf20204d582e2ca8f4736b0fb1fddd1e64e2c5041161b89c85b0b949fb1b367288192
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 3a09af338ff37fd4bd17ea15013baa92a8128f0d70d0a30b69278d6e8de6d114
```

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.ACCESS_DOWNLOAD_MANAGER	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_DOWNLOAD_MANAGER_ADVANCED	unknown	Unknown permission	Unknown permission from android reference
android.permission.REQUEST_INSTALL_PACKAGES	dangerous	Allows an application to request installing packages.	Malicious applications can use this to try and trick users into installing additional malicious packages.
android.permission.QUERY_ALL_PACKAGES	normal		Allows query of any normal app on the device, regardless of manifest declarations.
android.permission.MANAGE_EXTERNAL_STORAGE	dangerous	Allows an application a broad access to external storage in scoped storage	Allows an application a broad access to external storage in scoped storage. Intended to be used by few apps that need to manage files on behalf of the users.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.c2dm.permission.RECEIVE	signature	C2DM permissions	Permission for cloud to device messaging.
android.permission.REQUEST_DELETE_PACKAGES	normal		Allows an application to request deleting packages.
android.permission.DOWNLOAD_WITHOUT_NOTIFICATION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>r8 (possible dexmerge)</td></tr>
<tr><td>Manipulator Found</td><td>dexmerge</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes2.dex</td><td><table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr></table></td></tr>
<tr><td>classes3.dex</td><td><table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Compiler</td><td>r8</td></tr></table></td></tr>
<tr><td>classes4.dex</td><td><table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr></table></td></tr>
</table>

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	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.

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.
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 (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [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 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.

CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/unity3d/ads/UnityAds.java com/unity3d/ads/UnityAdsBaseOptions.java com/unity3d/ads/metadata/InAppPurchaseMetaData.java com/unity3d/ads/metadata/MetaData.java com/unity3d/services/UnityServices.java com/unity3d/services/ads/UnityAdsImplementation.java com/unity3d/services/ads/adunit/AdUnitActivity.java com/unity3d/services/ads/adunit/VideoPlayerHandler.java com/unity3d/services/ads/api/AdUnit.java com/unity3d/services/ads/api/VideoPlayer.java com/unity3d/services/ads/api/WebPlayer.java com/unity3d/services/ads/configuration/AdsModuleConfiguration.java com/unity3d/services/ads/video/VideoPlayerView.java com/unity3d/services/ads/webplayer/WebPlayerView.java com/unity3d/services/ar/ARUtils.java com/unity3d/services/ar/view/ARView.java com/unity3d/services/ar/view/GLSurfaceView.java com/unity3d/services/ar/view/ShaderLoader.java com/unity3d/services/banners/BannerView.java com/unity3d/services/banners/UnityBanners.java com/unity3d/services/core/api/Cache.java com/unity3d/services/core/api/DeviceInfo.java com/unity3d/services/core/api/Intent.java com/unity3d/services/core/api/Request.java com/unity3d/services/core/api/Sdk.java com/unity3d/services/core/broadcast/BroadcastEventReceiver.java com/unity3d/services/core/cache/CacheDirectory.java com/unity3d/services/core/cache/CacheThread.java com/unity3d/services/core/cache/CacheThreadHand

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	ler.java com/unity3d/services/core/configuration/Configuration.java com/unity3d/services/core/configuration/EnvironmentCheck.java com/unity3d/services/core/configuration/InitializationNotificationCenter.java com/unity3d/services/core/configuration/InitializeThread.java com/unity3d/services/core/connectivity/ConnectivityMonitor.java com/unity3d/services/core/device/AdvertisingId.java com/unity3d/services/core/device/Device.java com/unity3d/services/core/device/OpenAdvertisingId.java com/unity3d/services/core/device/Storage.java com/unity3d/services/core/log/DeviceLog.java com/unity3d/services/core/misc/JsonStorage.java com/unity3d/services/core/misc/Utilities.java com/unity3d/services/core/misc/ViewUtilities.java com/unity3d/services/core/preferences/AndroidPreferences.java com/unity3d/services/core/properties/ClientProperties.java com/unity3d/services/core/properties/SdkProperties.java com/unity3d/services/core/request/SDKMetrics.java com/unity3d/services/core/request/WebRequest.java com/unity3d/services/core/request/WebRequestRunnable.java com/unity3d/services/core/request/WebRequestThread.java com/unity3d/services/core/sensorinfo/SensorInfoListener.java com/unity3d/services/core/webview/WebView.java com/unity3d/services/core/webview/WebViewApp.java com/unity3d/services/core/webview/bridge/Invocation.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/unity3d/services/core/webview/bridge/NativeCallback.java com/unity3d/services/core/webview/bridge/WebViewBridge.java com/unity3d/services/core/webview/bridge/WebViewBridgeInterface.java com/unity3d/services/core/webview/bridge/WebViewCallback.java com/unity3d/services/monetization/UnityMonetization.java com/unity3d/services/monetization/core/utilities/JSONUtilities.java com/unity3d/services/monetization/placementcontent/core/PlacementContent.java com/unity3d/services/purchasing/core/TransactionDetailsUtilities.java com/unity3d/services/purchasing/core/TransactionErrorDetailsUtilities.java com/unity3d/services/purchasing/core/api/CustomPurchasing.java com/unity3d/services/store/StoreBilling.java
2	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	com/unity3d/services/ads/webplayer/WebPlayerView.java com/unity3d/services/core/webview/WebView.java
3	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	com/xc3fff0e/xmanager/oq.java com/xc3fff0e/xmanager/pz.java com/xc3fff0e/xmanager/rg.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	com/unity3d/services/core/device/Device.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	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	com/unity3d/ads/metadata/InAppPurchaseMetaData.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	com/unity3d/services/core/request/SDKMetrics.java com/xc3fff0e/xmanager/rk.java
7	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	com/unity3d/services/core/cache/CacheDirectory.java com/xc3fff0e/xmanager/b.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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
3	FCS_CKM_EXT.1.1	Security Functional Requirements	Cryptographic Key Generation Services	The application implement asymmetric key generation.
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.
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_CKM.1.1(1)	Selection-Based Security Functional Requirements	Cryptographic Asymmetric Key Generation	The application generate asymmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm RSA schemes using cryptographic key sizes of 2048-bit or greater.
11	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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
12	FCS_HTTPS_EXT.1.1	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement the HTTPS protocol that complies with RFC 2818.
13	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.
14	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.
15	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.
16	FPT_TUD_EXT.2.1	Selection-Based Security Functional Requirements	Integrity for Installation and Update	The application shall be distributed using the format of the platform-supported package manager.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION

DOMAIN	STATUS	GEOLOCATION
config.unityads.unity3d.com	ok	**IP:** 23.223.200.152 **Country:** United States of America **Region:** Georgia **City:** Atlanta **Latitude:** 33.749001 **Longitude:** -84.387978 **View:** Google Map
config.unityads.unitychina.cn	ok	**IP:** 222.143.140.97 **Country:** China **Region:** Henan **City:** Hebi **Latitude:** 35.899170 **Longitude:** 114.192497 **View:** Google Map
xmanager.firebaseio.com	ok	**IP:** 34.120.160.131 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://xmanager.firebaseio.com	info App talks to a Firebase Database.

TRACKERS

TRACKER	CATEGORIES	URL
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Unity3d Ads	Advertisement	https://reports.exodus-privacy.eu.org/trackers/121

HARDCODED SECRETS

POSSIBLE SECRETS
"firebase_database_url" : "https://xmanager.firebaseio.com"
"google_api_key" : "AIzaSyA-VMxSPY-pE8IikR3BZVFgBvthhZPT1Js"

Report Generated by - MobSF v3.6.2 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.