ANDROID STATIC ANALYSIS REPORT

Aruba Networks Login (0.5)

File Name:	installer351.apk
Package Name:	io.mkg20001.arubanetworkslogin
Scan Date:	May 31, 2022, 3:15 p.m.
App Security Score:	**66/100 (LOW RISK)**
Grade:	**A**

⬤ FINDINGS SEVERITY

🐛 HIGH	⚠ MEDIUM	ℹ INFO	✔ SECURE	🔍 HOTSPOT
1	6	1	3	1

📦 FILE INFORMATION

File Name: installer351.apk
Size: 2.54MB
MD5: 5373b7a120d07eeabfc1db4aa3fba30e
SHA1: e3890592a1f1911a885405289eeb01d106079f94
SHA256: c071cc04745beeb6c72e6563dbe99ecb8d92a94c780e513ee0c36c3ffc0c3343

ℹ APP INFORMATION

App Name: Aruba Networks Login
Package Name: io.mkg20001.arubanetworkslogin
Main Activity: io.mkg20001.arubanetworkslogin.LoginActivity
Target SDK: 28
Min SDK: 15
Max SDK:
Android Version Name: 0.5
Android Version Code: 5000

▦ APP COMPONENTS

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

✿ CERTIFICATE INFORMATION

Failed to read Code Signing Certificate or none available.

☰ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.
android.permission.READ_PROFILE	dangerous	read the user's personal profile data	Allows an application to read the user's personal profile data.
android.permission.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.

PERMISSION	STATUS	INFO	DESCRIPTION
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.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.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.

APKID ANALYSIS

FILE	DETAILS

FILE	DETAILS
classes.dex	**FINDINGS** — **DETAILS** table below

FINDINGS	DETAILS
Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.BRAND check Build.DEVICE check Build.PRODUCT check Build.TAGS check possible VM check
Compiler	r8 without marker (suspicious)

🔒 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.
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 (io.mkg20001.arubanetworkslogin.WifiReceiver) 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.
4	Service (io.mkg20001.arubanetworkslogin.WifiService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_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.

</> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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	io/sentry/connection/RandomEventSampler.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	io/sentry/event/interfaces/UserInterface.java io/sentry/marshaller/json/UserInterfaceBinding.java
3	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	io/mkg20001/arubanetworkslogin/WifiReceiver.java org/slf4j/helpers/Util.java io/sentry/android/event/helper/AndroidEventBuilderHelper.java io/sentry/android/AndroidSentryClientFactory.java io/mkg20001/arubanetworkslogin/WifiService.java io/mkg20001/arubanetworkslogin/Utils.java io/mkg20001/arubanetworkslogin/CaptiveLoginTask.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	io/sentry/android/event/helper/AndroidEventBuilderHelper.java
5	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	io/sentry/android/event/helper/AndroidEventBuilderHelper.java
6	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	io/mkg20001/arubanetworkslogin/UtilsJava.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 invoke platform-provided 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 ['address book'].
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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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_RBG_EXT.2.1,FCS_RBG_EXT.2.2	Selection-Based Security Functional Requirements	Random Bit Generation from Application	The application perform all deterministic random bit generation (DRBG) services in accordance with NIST Special Publication 800-90A using Hash_DRBG. The deterministic RBG is seeded by an entropy source that accumulates entropy from a platform-based DRBG and a software-based noise source, with a minimum of 256 bits of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.
11	FCS_HTTPS_EXT.1.1	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement the HTTPS protocol that complies with RFC 2818.
12	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.
13	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.
14	FIA_X509_EXT.1.1	Selection-Based Security Functional Requirements	X.509 Certificate Validation	The application invoked platform-provided functionality to validate certificates in accordance with the following rules: ['The certificate path must terminate with a trusted CA certificate'].
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.

🔍 DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
www.slf4j.org	ok	**IP:** 83.173.251.158 **Country:** Switzerland **Region:** Zurich **City:** Zurich **Latitude:** 47.366669 **Longitude:** 8.550000 **View:** [Google Map](#)
sentry.io	ok	**IP:** 35.188.42.15 **Country:** United States of America **Region:** Iowa **City:** Council Bluffs **Latitude:** 41.261940 **Longitude:** -95.860832 **View:** [Google Map](#)
detectportal.firefox.com	ok	**IP:** 34.107.221.82 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** [Google Map](#)
docs.sentry.io	ok	**IP:** 76.76.21.164 **Country:** United States of America **Region:** California **City:** Walnut **Latitude:** 34.015400 **Longitude:** -117.858223 **View:** [Google Map](#)

✉ EMAILS

EMAIL	FILE
4fb5be10fc429bc5e2a0@sentry.io	io/mkg20001/arubanetworkslogin/LoginActivity.java
4fb5be10fc429bc5e2a0@sentry.io	io/mkg20001/arubanetworkslogin/WifiReceiver.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.