MOBSF

ANDROID STATIC ANALYSIS REPORT

RIT Mobile (4.1)

File Name:	RIT_Mobile_4.1_APKPure.apk
Package Name:	edu.rit.ritmobile
Scan Date:	Feb. 6, 2025, 1:50 a.m.
App Security Score:	45/100 (MEDIUM RISK)
Grade:	
Trackers Detection:	1/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
3	14	2	1	1

FILE INFORMATION

File Name: RIT_Mobile_4.1_APKPure.apk
Size: 3.7MB
MD5: 94def3b50b8b967261bcabfe13d2d753
SHA1: d7f2ed50da7a19984cb0af3470f2493fe7871885
SHA256: 04ad1dbe066ca64131086e48231faf406209752e9421f25f2ee3e5add40a10bb

APP INFORMATION

App Name: RIT Mobile
Package Name: edu.rit.ritmobile
Main Activity: modolabs.kurogo.activity.ModuleActivity
Target SDK: 31
Min SDK: 24
Max SDK:
Android Version Name: 4.1

Android Version Code: 38

APP COMPONENTS

Activities: 8
Services: 11
Receivers: 9
Providers: 5
Exported Activities: 1
Exported Services: 1
Exported Receivers: 2
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: C=NY, ST=New York, L=Rochester, O=Rochester Institute of Technology, OU=Information & Technology Services, CN=RIT ITS
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2011-11-30 14:39:20+00:00
Valid To: 2039-04-17 14:39:20+00:00
Issuer: C=NY, ST=New York, L=Rochester, O=Rochester Institute of Technology, OU=Information & Technology Services, CN=RIT ITS
Serial Number: 0x4ed64018
Hash Algorithm: sha1
md5: 52da1f65e3e610a9ecf8595280028f81
sha1: 3e89839ab08ef7f31dc6a30f9b8c59c38f6ea108
sha256: 9bbba22bb0dc1c9b5c2364843068c642b7b584152f477a220c7740cde48ac7fc
sha512: e4c1cb0bd2a4237e20ef523f7dceb97f7a54c16320d6cbdd4b6271f1429b089dcb0a731b9c6ebae8f6566c3f07ba9e0f82dc7db0e4a065b0c3cfa512b17a0d99
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 8d43616a1da551e8b70f34d700d94a04812cf6e0dad7b40647ba03055609aca1
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
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	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.

APKID ANALYSIS

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

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
modolabs.kurogo.activity.ModuleActivity	Schemes: http://, https://, edu.rit.ritmobile://, Hosts: m.rit.edu,
modolabs.kurogo.activity.LoginActivity	Schemes: kurogo://, Hosts: auth, Paths: /,

NETWORK SECURITY

HIGH: **1** | WARNING: **0** | INFO: **0** | SECURE: **0**

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	high	Base config is insecurely configured to permit clear text traffic to all domains.

CERTIFICATE ANALYSIS

HIGH: **0** | WARNING: **1** | INFO: **1**

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Certificate algorithm might be vulnerable to hash collision	warning	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues. The manifest file indicates SHA256withRSA is in use.

MANIFEST ANALYSIS

HIGH: **1** | WARNING: **4** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 7.0, [minSdk=24]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.
3	Activity (modolabs.kurogo.activity.LoginActivity) is not Protected. [android:exported=true]	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.
4	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.

NO	ISSUE	SEVERITY	DESCRIPTION
5	Service (androidx.work.impl.background.systemjob.SystemJobService) 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.
6	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [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

HIGH: 1 | WARNING: 7 | INFO: 2 | SECURE: 1 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a1/b.java a2/e.java a4/a.java b/a.java b1/b.java b4/g.java b7/d.java c/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				c/e.java c/i.java c/q.java c2/j.java c9/c.java com/bumptech/glide/b.java com/parse/ConnectivityNotifier.java com/parse/InstallationId.java com/parse/ManifestInfo.java com/parse/NetworkQueryController.java com/parse/Parse.java com/parse/ParseDateFormat.java com/parse/ParseImpreciseDateFormat.java com/parse/ParseInstallation.java com/parse/ParseKeyValueCache.java com/parse/ParseObject.java com/parse/ParsePinningEventuallyQueue.java com/parse/ParseRequest.java d2/a.java e2/j.java e2/k.java e2/m.java e2/z.java f2/i.java f2/j.java f8/e.java g/f.java g2/e.java g2/j.java g3/d.java g3/e.java g3/h.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	g3/m.java g5/c.java h0/a.java h0/b.java h0/g.java h0/n.java h0/u.java h2/a.java i1/b.java i2/s.java i3/b0.java i3/c.java i3/e0.java i3/o1.java i3/q.java i3/q0.java i3/u.java i3/z0.java j3/b.java j3/e.java j3/f.java j3/g.java j3/i.java j3/i0.java j3/k.java j3/n.java k0/b.java k5/b.java k5/c0.java k5/e0.java k5/f.java k5/f0.java k5/h.java k5/i.java k5/j0.java k5/k.java k5/k0.java k5/m.java k5/n.java k5/o.java k5/q.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				k5/s.java k5/v.java k9/h.java l1/k.java l2/c.java l2/k.java l2/l.java l2/p.java l2/t.java l9/d.java m0/c.java m3/a.java n3/f.java o5/e.java o5/g.java p/d.java p0/a.java p2/a.java p2/i.java p5/c.java q/e.java q2/b.java r2/d.java r2/i.java r2/j.java r2/m.java s/b.java s/d.java s4/c.java t3/f.java u2/g.java u3/t.java v0/e.java v6/d.java w/b.java w/c.java w/e.java w4/a.java x0/f.java x0/g.java x0/j.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				x3/a.java y0/a.java y3/a.java y4/f.java z/e.java z/f.java z/g.java z/h.java z/l.java z1/a.java z2/a.java z3/l.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	e2/q.java u6/h0.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	b1/a.java com/parse/OfflineSQLiteOpenHelper.java com/parse/ParseSQLiteDatabase.java
4	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	k9/c.java k9/d.java k9/g.java k9/h.java
5	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/parse/ParseCommandCache.java v8/l.java x0/j.java
6	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	k5/i.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	com/parse/LocalIdManager.java g6/a.java g6/b.java h6/a.java
8	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	com/parse/ParseDigestUtils.java com/parse/ParseRESTCommand.java
9	The App uses ECB mode in Cryptographic encryption algorithm. ECB mode is known to be weak as it results in the same ciphertext for identical blocks of plaintext.	high	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-2	modolabs/kurogo/login/EncryptService.java
10	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	u7/o0.java
11	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	w7/b.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	a8/b.java a8/h.java e7/q.java f7/a.java g3/e.java j8/e.java modolabs/kurogo/activity/ErrorActivity.java modolabs/kurogo/activity/TabLoginActivity.java o5/e.java s/d.java v8/i.java v8/l.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	a8/b.java e7/q.java g3/e.java j8/e.java modolabs/kurogo/activity/TabLoginActivity.java o5/e.java
00137	Get last known location of the device	location collection	c/i.java p8/c.java
00115	Get last known location of the device	collection location	c/i.java p8/c.java
00036	Get resource file from res/raw directory	reflection	g3/e.java o5/e.java z6/a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00091	Retrieve data from broadcast	collection	j8/e.java modolabs/kurogo/activity/ErrorActivity.java modolabs/kurogo/activity/ModuleActivity.java modolabs/kurogo/activity/NotificationActivity.java modolabs/kurogo/activity/TabLoginActivity.java modolabs/kurogo/content/KurogoContentActivity.java modolabs/kurogo/login/EncryptService.java
00013	Read file and put it into a stream	file	com/fasterxml/jackson/core/JsonFactory.java com/parse/ParseCountingFileHttpBody.java com/parse/ParseFileHttpBody.java com/parse/ParseFileUtils.java i2/e.java j9/a.java k5/f0.java p0/a.java x0/j.java z/f.java z/g.java z/l.java z0/b.java z1/a.java
00022	Open a file from given absolute path of the file	file	b1/b.java com/fasterxml/jackson/databind/ser/std/FileSerializer.java e7/h.java s5/s.java v8/i.java v8/l.java x0/j.java z0/a.java
00023	Start another application from current application	reflection control	v8/l.java

RULE ID	BEHAVIOUR	LABEL	FILES
00114	Create a secure socket connection to the proxy address	network command	f9/i.java
00112	Get the date of the calendar event	collection calendar	com/fasterxml/jackson/databind/ser/std/StdKeySerializers.java com/fasterxml/jackson/databind/util/StdDateFormat.java
00012	Read data and put it into a buffer stream	file	p0/a.java
00191	Get messages in the SMS inbox	sms	f7/a.java v8/i.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	d2/a.java s5/q.java
00162	Create InetSocketAddress object and connecting to it	socket	k9/b.java k9/h.java
00163	Create new Socket and connecting to it	socket	k9/b.java k9/h.java
00089	Connect to a URL and receive input stream from the server	command network	c2/j.java
00030	Connect to the remote server through the given URL	network	c2/j.java
00109	Connect to a URL and get the response code	network command	c2/j.java
00016	Get location info of the device and put it to JSON object	location collection	l7/f.java

RULE ID	BEHAVIOUR	LABEL	FILES
00094	Connect to a URL and read data from it	command network	o5/g.java
00009	Put data in cursor to JSON object	file	com/parse/OfflineStore.java
00147	Get the time of current location	collection location	c/i.java
00075	Get location of the device	collection location	c/i.java

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	7/25	android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION, android.permission.INTERNET, android.permission.CAMERA, android.permission.WAKE_LOCK, android.permission.RECEIVE_BOOT_COMPLETED
Other Common Permissions	2/44	com.google.android.c2dm.permission.RECEIVE, android.permission.FOREGROUND_SERVICE

Malware Permissions:
Top permissions that are widely abused by known malware.
Other Common Permissions:
Permissions that are commonly abused by known malware.

OFAC SANCTIONED COUNTRIES

This app may communicate with the following OFAC sanctioned list of countries.

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
www.example.com	ok	**IP:** 23.223.209.216 **Country:** France **Region:** Ile-de-France **City:** Aubervilliers **Latitude:** 48.916672 **Longitude:** 2.383330 **View:** Google Map
github.com	ok	**IP:** 140.82.112.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
plus.google.com	ok	**IP:** 142.250.81.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

EMAILS

EMAIL	FILE
u0013android@android.com u0013android@android.com0	g3/r.java

TRACKERS

TRACKER	CATEGORIES	URL
Bolts	Analytics	https://reports.exodus-privacy.eu.org/trackers/403

HARDCODED SECRETS

POSSIBLE SECRETS
"enable_logging_preference_key" : "enable_logging"
49f946663a8deb7054212b8adda248c6
c103703e120ae8cc73c9248622f3cd1e

PLAYSTORE INFORMATION

Title: RIT Mobile

Score: 2.8333333 **Installs:** 10,000+ **Price:** 0 **Android Version Support:** **Category:** Education **Play Store URL:** edu.rit.ritmobile

Developer Details: Rochester Institute of Technology, Rochester+Institute+of+Technology, 1 Lomb Memorial Dr, Rochester, NY 14623, http://www.rit.edu/its/help, webmaster@rit.edu,

Release Date: Dec 5, 2011 **Privacy Policy:** Privacy link

Description:

RIT Mobile brings essential information and services to Android users: •Real-time bus locations, next arrival times, and schedules •Open/Closed RIT dining locations with menus, hours and days of service •Searchable RIT campus map •Calendar of RIT campus events displayed by date or category •RIT news from the University News office •RIT Athletics news, and schedules for individual Men's and Women's sports •Links to RIT Tiger Center, Tiger Bucks, Reporter Magazine, Wallace Library, Tickets, and Academic Calendar •RIT Photos •RIT Videos •RIT Twitter and Facebook postings •Lab hours and locations •Customizable homepage •Bookmark favorite links •Access to the full RIT website

SCAN LOGS

Timestamp	Event	Error
2025-02-06 01:50:38	Generating Hashes	OK
2025-02-06 01:50:38	Extracting APK	OK
2025-02-06 01:50:38	Unzipping	OK
2025-02-06 01:50:39	Parsing APK with androguard	OK
2025-02-06 01:50:39	Extracting APK features using aapt/aapt2	OK

2025-02-06 01:50:39	Getting Hardcoded Certificates/Keystores	OK
2025-02-06 01:50:43	Parsing AndroidManifest.xml	OK
2025-02-06 01:50:43	Extracting Manifest Data	OK
2025-02-06 01:50:43	Manifest Analysis Started	OK
2025-02-06 01:50:44	Reading Network Security config from network_security_config.xml	OK
2025-02-06 01:50:44	Parsing Network Security config	OK
2025-02-06 01:50:44	Performing Static Analysis on: RIT Mobile (edu.rit.ritmobile)	OK
2025-02-06 01:50:44	Fetching Details from Play Store: edu.rit.ritmobile	OK
2025-02-06 01:50:44	Checking for Malware Permissions	OK
2025-02-06 01:50:44	Fetching icon path	OK
2025-02-06 01:50:44	Library Binary Analysis Started	OK

2025-02-06 01:50:44	Reading Code Signing Certificate	OK
2025-02-06 01:50:46	Running APKiD 2.1.5	OK
2025-02-06 01:50:49	Updating Trackers Database....	OK
2025-02-06 01:50:49	Detecting Trackers	OK
2025-02-06 01:50:51	Decompiling APK to Java with JADX	OK
2025-02-06 01:51:18	Converting DEX to Smali	OK
2025-02-06 01:51:18	Code Analysis Started on - java_source	OK
2025-02-06 01:51:24	Android SBOM Analysis Completed	OK
2025-02-06 01:51:28	Android SAST Completed	OK
2025-02-06 01:51:28	Android API Analysis Started	OK
2025-02-06 01:51:31	Android API Analysis Completed	OK

2025-02-06 01:51:32	Android Permission Mapping Started	OK
2025-02-06 01:51:36	Android Permission Mapping Completed	OK
2025-02-06 01:51:36	Android Behaviour Analysis Started	OK
2025-02-06 01:51:43	Android Behaviour Analysis Completed	OK
2025-02-06 01:51:43	Extracting Emails and URLs from Source Code	OK
2025-02-06 01:51:45	Email and URL Extraction Completed	OK
2025-02-06 01:51:45	Extracting String data from APK	OK
2025-02-06 01:51:45	Extracting String data from Code	OK
2025-02-06 01:51:45	Extracting String values and entropies from Code	OK
2025-02-06 01:51:47	Performing Malware check on extracted domains	OK
2025-02-06 01:51:48	Saving to Database	OK

Report Generated by - MobSF v4.3.0

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.