ANDROID STATIC ANALYSIS REPORT

RIT Mobile (4.0)

File Name:	RIT Mobile_v4.0_apkpure.com.apk
Package Name:	edu.rit.ritmobile
Average CVSS Score:	6.4
App Security Score:	55/100 (MEDIUM RISK)
Scan Date:	Sept. 7, 2021, 7:11 p.m.

FILE INFORMATION

File Name: RIT Mobile_v4.0_apkpure.com.apk
Size: 2.97MB
MD5: d9e3121f6a2cf9f82a265c2599b461c5
SHA1: 4c7ca08b51e497797b47ed600cef0aec4fd7ffc6
SHA256: f43253213f9f1e649bcad6949addaaefb7ab76e6a783584a2f4f1e6a85e619d8

APP INFORMATION

App Name: RIT Mobile
Package Name: edu.rit.ritmobile
Main Activity: modolabs.kurogo.activity.ModuleActivity
Target SDK: 29
Min SDK: 21
Max SDK:
Android Version Name: 4.0
Android Version Code: 34

APP COMPONENTS

Activities: 7
Services: 7
Receivers: 1
Providers: 4
Exported Activities: 4
Exported Services: 3
Exported Receivers: 1
Exported Providers: 0

CERTIFICATE INFORMATION

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
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

STATUS	DESCRIPTION
secure	Application is signed with a code signing certificate
warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android <7.0
warning	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues. The manifest file indicates SHA256withRSA is in use.

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.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.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.
com.google.android.c2dm.permission.RECEIVE	signature	C2DM permissions	Permission for cloud to device messaging.
android.permission.USE_BIOMETRIC	normal		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.

APKID ANALYSIS

FILE	DETAILS
classes.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Compiler</td><td>r8</td></tr></table>

BROWSABLE ACTIVITIES

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

NETWORK SECURITY

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

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	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.
2	Activity (modolabs.kurogo.activity.ErrorActivity) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
3	Activity (modolabs.kurogo.activity.TabLoginActivity) is not Protected. [android:exported=true]	high	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	Activity (modolabs.kurogo.activity.LoginActivity) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
5	Service (modolabs.kurogo.login.KeepAliveService) is not Protected. [android:exported=true]	high	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
6	Service (com.google.firebase.messaging.FirebaseMessagingService) is not Protected. [android:exported=true]	high	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
7	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]	high	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.
8	Service (com.google.firebase.iid.FirebaseInstanceIdService) is not Protected. [android:exported=true]	high	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
9	Activity (androidx.biometric.DeviceCredentialHandlerActivity) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

</> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
				h/a/m/i.java h/a/l/e.java e/b/p/o0.java h/a/a0/b/n.java f/c/a/a/e/c/o.java f/c/a/a/c/l/f.java f/c/a/a/c/d.java e/b/o/i/g.java e/i/l/c.java f/c/b/g/l.java e/b/p/l0.java h/a/f0/d.java e/i/j/b.java h/a/l/o.java h/a/f0/a.java f/c/a/a/c/k/k/m0.java h/a/m/n.java h/a/w/b.java e/d/g.java e/b/k/c.java f/c/a/a/g/b/a.java e/i/j/n.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CVSS V2: 7.5 (high) CWE: CWE-532 Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	h/a/h0/g.java h/a/f0/i.java f/c/a/a/c/r.java h/a/w/e.java e/n/a/e.java f/c/a/a/c/k/k/s.java f/c/b/g/g0.java h/a/m/o.java e/i/l/d.java f/c/a/a/c/k/k/f2.java h/a/n/k.java h/a/f0/e.java h/a/m/s.java f/c/b/g/n.java e/i/l/b.java f/c/b/g/e.java e/k/b/a.java f/c/a/a/c/s.java e/i/l/e.java e/i/s/b.java f/c/b/g/q.java h/a/i0/a.java f/c/a/a/e/c/f.java f/c/a/a/e/d/r.java h/a/w/m.java e/b/p/w.java modolabs/kurogo/webview/KgouiWebView.java f/c/a/a/c/l/f0.java f/c/a/a/c/k/k/y1.java e/b/p/s0.java f/c/b/b.java e/i/s/g.java h/a/z/g.java h/a/a0/b/p.java f/c/b/g/x.java e/n/a/k.java h/a/i0/n.java h/a/m/g.java e/p/a/a.java h/a/m/f.java h/a/h0/j.java h/a/r/a.java h/a/h0/c.java f/c/b/g/a0.java h/a/w/g.java f/c/a/a/c/k/k/h1.java h/a/a0/b/h.java f/c/b/e/f.java h/a/d0/a.java f/c/a/a/c/l/a.java f/c/b/g/v.java f/c/a/a/c/g.java h/a/h0/h.java modolabs/kurogo/login/EncryptServiceV23.java f/c/b/g/i0.java modolabs/kurogo/activity/ModuleActivity.java f/c/a/a/c/l/i.java h/a/f0/g.java f/c/a/a/c/k/k/a0.java e/b/l/a/a.java h/a/w/h.java h/a/d0/b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				f/c/a/a/c/m/a.java f/c/b/g/a.java f/c/b/g/t.java e/m/a/a.java f/c/b/g/g.java f/c/b/g/z.java h/a/i0/d.java h/a/h0/i.java f/c/a/a/c/l/e.java e/d/b.java e/i/l/f.java e/l/d.java f/c/b/g/y.java h/a/h0/b.java e/x/v.java e/b/p/b1.java e/d/e.java h/a/l/j.java f/c/a/b/j/g.java h/a/h0/e.java h/a/t/b.java e/b/k/p.java e/i/s/p.java modolabs/kurogo/activity/NotificationActivity.java h/a/m/t.java h/a/e0/a.java f/c/b/g/j0.java e/b/p/a0.java h/a/m/j.java f/c/a/a/e/c/a.java h/a/i0/g.java f/c/a/a/c/k/k/d1.java h/a/i0/f.java f/c/a/a/c/k/k/p1.java h/a/z/h.java d/a/b/a/a.java h/a/w/c.java f/c/a/a/c/l/m.java h/a/e0/b.java f/c/b/g/h0.java h/a/m/l.java f/c/a/a/c/k/k/d.java f/c/b/g/w0.java h/a/r/b.java e/u/c/p.java f/c/b/g/z0.java f/c/b/g/c0.java e/b/o/f.java e/i/l/i/d.java h/a/w/l.java modolabs/kurogo/login/EncryptService.java e/b/p/y0.java h/a/f0/j.java e/y/a/a/g.java h/a/a0/b/i.java f/c/a/a/c/l/b.java h/a/m/d.java f/c/a/a/c/k/k/h0.java f/c/a/a/c/h.java f/c/a/a/c/l/k0.java h/a/a0/b/b.java h/a/w/d.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	App creates temp file. Sensitive information should never be written into a temp file.	warning	CVSS V2: 5.5 (medium) CWE: CWE-276 Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	h/a/f0/e.java
3	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	CVSS V2: 0 (info) OWASP MASVS: MSTG-NETWORK-4	i/x.java
4	The App uses an insecure Random Number Generator.	warning	CVSS V2: 7.5 (high) CWE: CWE-330 Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	b/a/d2/b.java
5	Remote WebView debugging is enabled.	high	CVSS V2: 5.4 (medium) CWE: CWE-919 - Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	modolabs/kurogo/application/KurogoApplication.java
6	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	CVSS V2: 5.9 (medium) 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

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 implement asymmetric key generation.
4	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['network connectivity', 'location', 'camera'].
5	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to no sensitive information repositories.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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_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_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.
12	FCS_COP.1.1(1)	Selection-Based Security Functional Requirements	Cryptographic Operation - Encryption/Decryption	The application perform encryption/decryption not in accordance with FCS_COP.1.1(1), AES-ECB mode is being used.
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	FCS_CKM.1.1(2)	Optional Security Functional Requirements	Cryptographic Symmetric Key Generation	The application shall generate symmetric cryptographic keys using a Random Bit Generator as specified in FCS_RBG_EXT.1 and specified cryptographic key sizes 128 bit or 256 bit.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
plus.google.com	good	**IP:** 142.250.190.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
schemas.android.com	good	**IP:** 74.69.66.251 **Country:** United States of America **Region:** New York **City:** Rochester **Latitude:** 43.154781 **Longitude:** -77.615562 **View:** Google Map
www.example.com	good	**IP:** 93.184.216.34 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

URLS

URL	FILE
http://schemas.android.com/apk/res/android	d/a/b/a/a.java
https://plus.google.com/	f/c/a/a/c/l/h0.java
data:text	h/a/f0/j.java
http://www.example.com	h/a/z/g.java

EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	f/c/a/a/c/x.java

HARDCODED SECRETS

POSSIBLE SECRETS
"append_credentials" : "Please enter your credentials for"
"biometric_challenge_authentication_negative_button" : ""
"credentials" : "Please enter your credentials."
"pwd" : "Use Password"

PLAYSTORE INFORMATION

Title: RIT Mobile

Score: 3.54 **Installs:** 10,000+ **Price:** 0 **Android Version Support:** 5.0 and up **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

App Security Score Calculation

Every app is given an ideal score of 100 to begin with.
For every findings with severity high we reduce 15 from the score.
For every findings with severity warning we reduce 10 from the score.
For every findings with severity good we add 5 to the score.
If the calculated score is greater than 100, then the app security score is considered as 100.
And if the calculated score is less than 0, then the app security score is considered as 10.

Risk Calculation

APP SECURITY SCORE	RISK
0 - 15	CRITICAL
16 - 40	HIGH
41 - 70	MEDIUM
71 - 100	LOW

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.