MOBSF

ANDROID STATIC ANALYSIS REPORT

Tigersafe (1.5)

File Name:	Tigersafe RIT_v1.5_apkpure.com.apk
Package Name:	com.cutcom.apparmor.rit
Average CVSS Score:	6.7
App Security Score:	10/100 (CRITICAL RISK)
Trackers Detection:	2/405
Scan Date:	Sept. 7, 2021, 7:26 p.m.

FILE INFORMATION

File Name: Tigersafe RIT_v1.5_apkpure.com.apk
Size: 21.84MB
MD5: abb6673a71feb649de528f6df905fe5f
SHA1: 35676a028fd0467dc955dc98c7128a954252c789
SHA256: 05da42c1fb099b2b747fd3fcaabf7818382787ffe5dc9615c9e772fda0ebc83e

APP INFORMATION

App Name: Tigersafe
Package Name: com.cutcom.apparmor.rit
Main Activity: com.cutcom.apparmor.rit.TigersafeActivity
Target SDK: 29
Min SDK: 19
Max SDK:
Android Version Name: 1.5
Android Version Code: 15

APP COMPONENTS

Activities: 16
Services: 7
Receivers: 4
Providers: 2
Exported Activities: 8
Exported Services: 0
Exported Receivers: 2
Exported Providers: 0

CERTIFICATE INFORMATION

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=CA, ST=Ontario, L=Kingston, O=CutCom Software Inc., OU=Development, CN=Chris Sinkinson
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2011-03-29 03:59:42+00:00
Valid To: 2038-08-14 03:59:42+00:00
Issuer: C=CA, ST=Ontario, L=Kingston, O=CutCom Software Inc., OU=Development, CN=Chris Sinkinson
Serial Number: 0x4d91592e
Hash Algorithm: sha1
md5: d1523dbf7b3ab3aee7a246bd99f6be25
sha1: 525b932aef2d50a0a9633e0368ab1d7ecffb54d3
sha256: f34b0590731d17d225f8c7bdac1cd61302354f4d643fc82a256ef611c8504feb
sha512: cc50d494e65d0528b36ac9687e59829a8d71cfe7e14da8e5bcd59bf95cc0e9aa4037ba458a420aad29e778d7cd42668607ded20e088e4413c120416c8bcea3ff
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 91fc3b035aea0062fef707152381431be6e21ee10749a4480d490585eda626f5

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.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.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
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.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground.
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference
android.permission.FLASHLIGHT	normal	control flashlight	Allows the application to control the flashlight.
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.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.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.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
com.cutcom.apparmor.rit.permission.MAPS_RECEIVE	unknown	Unknown permission	Unknown permission from android reference
android.permission.CHANGE_WIFI_STATE	normal	change Wi-Fi status	Allows an application to connect to and disconnect from Wi-Fi access points and to make changes to configured Wi-Fi networks.
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.

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
Build.PRODUCT check
Build.HARDWARE check
Build.BOARD check
possible VM check</td></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
<tr><td>classes2.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>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.cutcom.apparmor.rit.TigersafeActivity	Schemes: tigersaferit://,
com.google.zxing.client.android.CaptureActivity	Schemes: http://, zxing://, Hosts: zxing.appspot.com, www.google.com, www.google.co.uk, scan, Paths: /scan, /m/products/scan, /,

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] flag is missing.	medium	The flag [android:allowBackup] should be set to false. By default it is set to true and 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.

NO	ISSUE	SEVERITY	DESCRIPTION
3	Broadcast Receiver (com.appcelerator.aps.PushBroadcastReceiver) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
4	Activity (com.google.zxing.client.android.CaptureActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.
5	Activity (com.google.zxing.client.android.encode.EncodeActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.
6	Activity (com.google.zxing.client.android.book.SearchBookContentsActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.
7	Activity (com.google.zxing.client.android.share.ShareActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.
8	Activity (com.google.zxing.client.android.history.HistoryActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.
9	Activity (com.google.zxing.client.android.share.BookmarkPickerActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.
10	Activity (com.google.zxing.client.android.share.AppPickerActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.
11	Activity (com.google.zxing.client.android.HelpActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.
12	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.

</> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
				org/appcelerator/kroll/common/TiDeployData.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ti/modules/titanium/ui/PickerProxy.java ti/modules/titanium/ui/TableViewRowProxy.java org/appcelerator/titanium/TiProperties.java ti/modules/titanium/ui/widget/TiUIDrawerLayout.java ti/modules/titanium/geolocation/android/AndroidModule.java ti/modules/titanium/network/socket/TCPProxy.java hyperloop/ProxyFactory.java org/appcelerator/kroll/util/KrollAssetHelper.java org/appcelerator/kroll/util/KrollAssetCache.java ti/map/PolylineProxy.java ti/modules/titanium/calendar/ReminderProxy.java ti/modules/titanium/ui/UIModule.java ti/modules/titanium/geolocation/GeolocationModule.java org/appcelerator/titanium/proxy/ActionBarProxy.java org/appcelerator/kroll/KrollRuntime.java ti/modules/titanium/codec/CodecModule.java ti/modules/titanium/media/AudioPlayerProxy.java ti/modules/titanium/network/NetworkModule.java org/appcelerator/titanium/proxy/TiWindowProxy.java ti/modules/titanium/network/NonValidatingSSLSocketFactory.java org/appcelerator/kroll/KrollProxy.java org/appcelerator/titanium/TiBaseActivity.java org/appcelerator/titanium/view/TiToolbarStyleHandler.java org/appcelerator/kroll/runtime/v8/V8Runtime.java ti/modules/titanium/android/TiJSService.java ti/barcode/FrontCamera.java org/appcelerator/kroll/util/TiTempFileHelper.java ti/modules/titanium/ui/widget/TiUIScrollableView.java com/appcelerator/aps/APSAnalytics.java org/appcelerator/kroll/common/Log.java org/appcelerator/titanium/proxy/ServiceProxy.java ti/modules/titanium/ui/widget/TiUIImageView.java ti/modules/titanium/ui/RefreshControlProxy.java org/appcelerator/titanium/TiApplication.java ti/modules/titanium/ui/_2DMatrixProxy.java ti/modules/titanium/android/notificationmanager/NotificationManagerModule.java ti/modules/titanium/ui/android/AndroidModule.java android/widget/TiVideoView8.java ti/modules/titanium/geolocation/TiLocation.java ti/modules/titanium/ui/widget/listview/TiListView.java ti/modules/titanium/media/SoundProxy.

NO	ISSUE	SEVERITY	STANDARDS	FILES
				java ti/modules/titanium/ui/widget/searchview/TiUISearchView.java com/appcelerator/aps/CloudpushModuleImplementation.java ti/modules/titanium/ui/widget/listview/ListSectionProxy.java ti/modules/titanium/ui/widget/TiUIButton.java ti/modules/titanium/ui/widget/TiUITabbedBar.java ti/modules/titanium/geolocation/android/LocationProviderProxy.java ti/modules/titanium/stream/BufferStreamProxy.java com/appcelerator/aps/APSAnalyticsMeta.java ti/modules/titanium/ui/widget/picker/TiUITimeSpinnerNumberPicker.java ti/modules/titanium/contacts/ContactsApiLevel5.java ti/modules/titanium/ui/widget/webview/TiUIWebView.java org/appcelerator/titanium/util/TiStreamHelper.java org/appcelerator/titanium/view/TiCompositeLayout.java com/cutcom/apparmor/rit/AssetCryptImpl.java org/appcelerator/titanium/view/TiActionBarStyleHandler.java ti/modules/titanium/android/quicksettings/QuickSettingsServiceProxy.java ti/modules/titanium/ui/ShortcutModule.java ti/modules/titanium/media/android/AndroidModule.java ti/modules/titanium/ui/ShortcutItemProxy.java ti/modules/titanium/ui/PickerRowProxy.java com/appcelerator/aps/APSAnalyticsStore.java ti/modules/titanium/calendar/RecurrenceRuleProxy.java ti/modules/titanium/ui/widget/TiUIDialog.java org/appcelerator/titanium/util/TiImageHelper.java ti/modules/titanium/ui/TableViewSectionProxy.java bencoding/android/tools/PlatformProxy.java org/appcelerator/titanium/proxy/MenuItemProxy.java ti/modules/titanium/ui/widget/tableview/TableViewModel.java ti/modules/titanium/geolocation/TiCompass.java ti/modules/titanium/ui/widget/TiImageView.java org/appcelerator/titanium/util/TiPlatformHelper.java ti/modules/titanium/android/notificationmanager/NotificationProxy.java org/appcelerator/titanium/TiVerify.java org/appcelerator/titanium/util/TiDownloadManager.java org/appcelerator/titanium/io/TiBaseFile.java ti/modules/titanium/network/TiNetworkListener.java org/appcelerator/titanium/view/TiBorde

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	org/appcelerator/titanium/view/TiBorderWrapperView.java ti/modules/titanium/database/DatabaseModule.java ti/modules/titanium/ui/widget/tabgroup/TiUIBottomNavigationTabGroup.java ti/modules/titanium/xml/XPathUtil.java org/appcelerator/titanium/proxy/IntentProxy.java org/appcelerator/kroll/common/TiMessenger.java org/appcelerator/kroll/runtime/v8/JSDebugger.java ti/modules/titanium/ui/widget/tabgroup/TiUITabLayoutTabGroup.java ti/modules/titanium/analytics/AnalyticsModule.java ti/modules/titanium/ui/AttributedStringProxy.java org/appcelerator/titanium/proxy/TiViewProxy.java ti/modules/titanium/stream/FileStreamProxy.java ti/modules/titanium/android/notificationmanager/NotificationChannelProxy.java org/appcelerator/titanium/view/TiBackgroundColorWrapper.java com/appcelerator/aps/APSProperties.java ti/modules/titanium/ui/widget/picker/TiUISpinnerColumn.java ti/modules/titanium/filesystem/FilesystemModule.java ti/modules/titanium/ui/widget/TiUILabel.java hyperloop/HyperloopModule.java org/appcelerator/kroll/runtime/v8/ReferenceTable.java ti/modules/titanium/ui/widget/TiUISlider.java ti/modules/titanium/android/TiJSIntervalService.java ti/modules/titanium/ui/widget/TiUIMaskedImage.java ti/modules/titanium/ui/widget/tabgroup/TiUIAbstractTabGroup.java org/appcelerator/titanium/proxy/DecorViewProxy.java ti/modules/titanium/media/TiCameraActivity.java org/appcelerator/titanium/proxy/ActivityProxy.java ti/modules/titanium/locale/DateTimeFormatProxy.java ti/modules/titanium/media/TiVideoActivity.java ti/modules/titanium/app/AndroidModule.java ti/modules/titanium/ui/EmailDialogProxy.java ti/modules/titanium/ui/android/TiPreferencesFragment.java com/codebutler/android_websockets/HybiParser.java com/cutcom/apparmor/rit/TigersafeApplication.java ti/modules/titanium/gesture/GestureModule.java org/appcelerator/kroll/KrollDict.java ti/modules/titanium/geolocation/android/FusedLocationProvider.java org/appcelerator/titanium/io/TiFile.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				org/appcelerator/titanium/TiFileProxy.java hyperloop/ClassProxy.java bencoding/android/Common.java com/codebutler/android_websockets/WebSocketClient.java ti/modules/titanium/database/TiResultSetProxy.java ti/modules/titanium/ui/widget/webview/TiWebViewClient.java ti/modules/titanium/ui/ScrollableViewProxy.java ti/modules/titanium/ui/widget/picker/TiUISpinner.java ti/modules/titanium/ui/widget/TiUINotification.java org/appcelerator/titanium/util/TiRHelper.java ti/modules/titanium/ui/widget/TiUIProgressIndicator.java org/appcelerator/titanium/util/TiFileHelper.java ti/modules/titanium/media/TiCamera.java ti/modules/titanium/ui/widget/TiUIActivityIndicator.java ti/modules/titanium/network/CookieProxy.java ti/modules/titanium/ui/widget/TiUIScrollView.java ti/modules/titanium/network/TiHTTPClient.java ti/modules/titanium/ui/clipboard/ClipboardModule.java ti/modules/titanium/ui/widget/tableview/TiTableViewRowProxyItem.java org/appcelerator/titanium/view/TiGradientDrawable.java ti/modules/titanium/utils/UtilsModule.java ti/modules/titanium/android/AndroidModule.java org/appcelerator/titanium/io/TiResourceFile.java org/appcelerator/titanium/view/TiUIView.java ti/modules/titanium/ui/widget/tableview/TiTableView.java org/appcelerator/titanium/proxy/MenuProxy.java com/appcelerator/aps/IntentReceiver.java ti/modules/titanium/gesture/TiDeviceOrientationMonitor.java org/appcelerator/titanium/TiStylesheet.java ti/modules/titanium/media/TiThumbnailRetriever.java ti/modules/titanium/locale/LocaleModule.java ti/modules/titanium/TitaniumModule.java hyperloop/InstanceProxy.java ti/modules/titanium/xml/XMLModule.java org/appcelerator/kroll/util/KrollStreamHelper.java org/appcelerator/titanium/util/TiActivitySupportHelper.java org/appcelerator/titanium/util/TiLoadImageManager.java org/appcelerator/titanium/io/TitaniumBlob.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/appcelerator/aps/CCPushService.java org/appcelerator/kroll/KrollLogging.java ti/modules/titanium/xml/NodeProxy.java ti/modules/titanium/ui/widget/picker/TiUITimeSpinner.java ti/barcode/BarcodeModule.java org/appcelerator/titanium/TiBaseService.java org/appcelerator/titanium/TiActivity.java org/appcelerator/titanium/util/TiColorHelper.java ti/modules/titanium/contacts/CommonContactsApi.java ti/map/TiMapInfoWindow.java ti/modules/titanium/ui/PickerColumnProxy.java ti/modules/titanium/ui/widget/listview/TiListViewTemplate.java org/appcelerator/kroll/runtime/v8/V8Function.java ti/map/AnnotationProxy.java com/appcelerator/aps/APSCloudPush.java ti/modules/titanium/BufferProxy.java com/appcelerator/aps/APSAnalyticsEvent.java ti/map/ViewProxy.java org/appcelerator/titanium/TiDimension.java ti/modules/titanium/calendar/EventProxy.java ti/modules/titanium/ui/widget/picker/TiUIDateSpinner.java com/nineoldandroids/animation/PropertyValuesHolder.java org/appcelerator/titanium/TiBlob.java ti/modules/titanium/ui/TabGroupProxy.java org/appcelerator/titanium/util/TiResponseCache.java com/appcelerator/aps/APSAnalyticsService.java ti/modules/titanium/ui/widget/webview/TiWebChromeClient.java ti/map/TiUIMapView.java ti/modules/titanium/app/AppModule.java ti/modules/titanium/media/TiSound.java ti/modules/titanium/contacts/PersonProxy.java org/appcelerator/titanium/util/TiUIHelper.java org/appcelerator/titanium/proxy/RProxy.java ti/modules/titanium/locale/NumberFormatProxy.java org/appcelerator/titanium/util/TiSensorHelper.java org/appcelerator/titanium/proxy/TiActivityWindowProxy.java org/appcelerator/titanium/TiLaunchActivity.java org/appcelerator/titanium/TiRootActivity.java ti/modules/titanium/ui/widget/listview/TiDefaultListViewTemplate.java ti/modules/titanium/ui/widget/picker/TiUINativePicker.java org/appcelerator/titanium/util/TiDigestUtils.java hyperloop/BaseProxy.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ti/modules/titanium/calendar/CalendarProxy.java org/java_websocket/AbstractWebSocket.java org/appcelerator/kroll/runtime/v8/V8Object.java org/appcelerator/titanium/TiExceptionHandler.java ti/modules/titanium/contacts/ContactsModule.java ti/modules/titanium/ui/widget/picker/CustomDatePicker.java ti/modules/titanium/database/TiDatabaseProxy.java ti/modules/titanium/ui/WindowProxy.java org/appcelerator/titanium/util/TiUrl.java org/appcelerator/titanium/view/TiDrawableReference.java org/appcelerator/titanium/util/TiLocationHelper.java hyperloop/InterfaceSubclassProxy.java ti/modules/titanium/ui/widget/TiUISwitch.java ti/modules/titanium/ui/widget/TiUITableView.java ti/modules/titanium/platform/PlatformModule.java ti/modules/titanium/ui/widget/webview/TiWebViewBinding.java hyperloop/HyperloopUtil.java ti/modules/titanium/media/VideoPlayerProxy.java ti/modules/titanium/ui/widget/tableview/TiBaseTableViewItem.java ti/light/TilightModule.java ti/modules/titanium/network/TiSocketFactory.java ti/modules/titanium/ui/WebViewProxy.java ti/map/TiClusterRenderer.java ti/modules/titanium/ui/widget/TiUIText.java ti/modules/titanium/ui/widget/picker/TiUIDatePicker.java ti/modules/titanium/android/notificationmanager/BigPictureStyleProxy.java net/iamyellow/tiws/WSProxy.java ti/modules/titanium/ui/LabelProxy.java ti/modules/titanium/ui/widget/listview/ListViewProxy.java ti/modules/titanium/media/MediaModule.java ti/modules/titanium/ui/widget/TiUICardView.java org/appcelerator/titanium/util/TiAnimationBuilder.java ti/modules/titanium/media/TiUIVideoView.java ti/modules/titanium/ui/TableViewProxy.java ti/modules/titanium/ui/widget/picker/TiUITimePicker.java org/appcelerator/titanium/util/TiConvert.java org/appcelerator/titanium/io/TiFileProvider.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CVSS V2: 7.4 (high) CWE: CWE-312 Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	ti/modules/titanium/ui/UIModule.java ti/modules/titanium/calendar/RecurrenceRuleProxy.java org/appcelerator/titanium/TiC.java ti/modules/titanium/ui/android/TiPreferencesActivity.java ti/modules/titanium/android/AndroidModule.java com/appcelerator/aps/PushConstants.java org/appcelerator/titanium/TiBaseService.java org/appcelerator/titanium/util/TiResponseCache.java
3	Insecure Implementation of SSL. Trusting all the certificates or accepting self signed certificates is a critical Security Hole. This application is vulnerable to MITM attacks	high	CVSS V2: 7.4 (high) CWE: CWE-295 Improper Certificate Validation OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	ti/modules/titanium/network/NonValidatingSSLSocketFactory.java ti/modules/titanium/network/TiHTTPClient.java
4	App can read/write to External Storage. Any App can read data written to External Storage.	high	CVSS V2: 5.5 (medium) CWE: CWE-276 Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	org/appcelerator/kroll/util/TiTempFileHelper.java ti/modules/titanium/filesystem/FilesystemModule.java ti/modules/titanium/android/EnvironmentModule.java org/appcelerator/titanium/util/TiFileHelper.java ti/modules/titanium/TitaniumModule.java ti/modules/titanium/ui/widget/webview/TiWebChromeClient.java ti/modules/titanium/media/MediaModule.java
5	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	org/appcelerator/kroll/util/TiTempFileHelper.java ti/modules/titanium/filesystem/FilesystemModule.java ti/modules/titanium/network/TiHTTPClient.java ti/modules/titanium/ui/widget/webview/TiWebChromeClient.java
6	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	ti/modules/titanium/ui/widget/webview/TiUIWebView.java
7	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CVSS V2: 7.4 (high) CWE: CWE-649 Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	com/cutcom/apparmor/rit/AssetCryptImpl.java
8	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	org/java_websocket/drafts/Draft_76.java org/java_websocket/drafts/Draft_75.java org/appcelerator/titanium/util/TiFileHelper.java ti/modules/titanium/network/httpurlconnection/HttpUrlConnectionUtils.java org/java_websocket/drafts/Draft_10.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
9	MD5 is a weak hash known to have hash collisions.	warning	CVSS V2: 7.4 (high) CWE: CWE-327 Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	org/java_websocket/drafts/Draft_76.java
10	SHA-1 is a weak hash known to have hash collisions.	warning	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-4	com/codebutler/android_websockets/WebSocketClient.java org/java_websocket/drafts/Draft_10.java
11	Insecure WebView Implementation. WebView ignores SSL Certificate errors and accept any SSL Certificate. This application is vulnerable to MITM attacks	high	CVSS V2: 7.4 (high) CWE: CWE-295 Improper Certificate Validation OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	ti/modules/titanium/ui/widget/webview/TiWebViewClient.java
12	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	ti/modules/titanium/network/TiHTTPClient.java
13	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	CVSS V2: 5.9 (medium) CWE: CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	ti/modules/titanium/database/TiDatabaseProxy.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	lib/arm64-v8a/libbencoding.android.tools.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	False info The shared object does not have run-time search path or RPATH set.	False info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	lib/arm64-v8a/libc++_shared.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	False info The shared object does not have run-time search path or RPATH set.	False info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	lib/arm64-v8a/libhyperloop.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	False info The shared object does not have run-time search path or RPATH set.	False info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	lib/arm64-v8a/libkroll-v8.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	False info The shared object does not have run-time search path or RPATH set.	False info The shared object does not have RUNPATH set.	True info The shared object has the following fortified functions: ['__memmove_chk', '__strlen_chk', '__fgets_chk', '__strchr_chk', '__memcpy_chk', '__vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	lib/arm64-v8a/libnet.iamyellow.tiws.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	False info The shared object does not have run-time search path or RPATH set.	False info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
6	lib/arm64-v8a/libti.barcode.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	False info The shared object does not have run-time search path or RPATH set.	False info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	lib/arm64-v8a/libti.cloak.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	False info The shared object does not have run-time search path or RPATH set.	False info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	lib/arm64-v8a/libti.cloudpush.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	False info The shared object does not have run-time search path or RPATH set.	False info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
9	lib/arm64-v8a/libti.light.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	False info The shared object does not have run-time search path or RPATH set.	False info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
10	lib/arm64-v8a/libti.map.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	False info The shared object does not have run-time search path or RPATH set.	False info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
11	lib/arm64-v8a/libti.playservices.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	False info The shared object does not have run-time search path or RPATH set.	False info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.
12	lib/armeabi-v7a/libbencoding.android.tools.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	False info The shared object does not have run-time search path or RPATH set.	False info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
13	lib/armeabi-v7a/libc++_shared.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	False info The shared object does not have run-time search path or RPATH set.	False info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.
14	lib/armeabi-v7a/libhyperloop.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	False info The shared object does not have run-time search path or RPATH set.	False info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
15	lib/armeabi-v7a/libkroll-v8.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	False info The shared object does not have run-time search path or RPATH set.	False info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.
16	lib/armeabi-v7a/libnet.iamyellow.tiws.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	False info The shared object does not have run-time search path or RPATH set.	False info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
17	lib/armeabi-v7a/libti.barcode.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	False info The shared object does not have run-time search path or RPATH set.	False info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.
18	lib/armeabi-v7a/libti.cloak.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	False info The shared object does not have run-time search path or RPATH set.	False info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
19	lib/armeabi-v7a/libti.cloudpush.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	False info The shared object does not have run-time search path or RPATH set.	False info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.
20	lib/armeabi-v7a/libti.light.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	False info The shared object does not have run-time search path or RPATH set.	False info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
21	lib/armeabi-v7a/libti.map.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	False info The shared object does not have run-time search path or RPATH set.	False info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.
22	lib/armeabi-v7a/libti.playservices.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	False info The shared object does not have run-time search path or RPATH set.	False info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.

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 invoke the functionality provided by the platform to securely store 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', 'location', 'camera'].
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_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_COP.1.1(1)	Selection-Based Security Functional Requirements	Cryptographic Operation - Encryption/Decryption	The application perform encryption/decryption in accordance with a specified cryptographic algorithm AES-CBC (as defined in NIST SP 800-38A) mode or AES-GCM (as defined in NIST SP 800-38D) and cryptographic key sizes 256-bit/128-bit.
12	FCS_COP.1.1(2)	Selection-Based Security Functional Requirements	Cryptographic Operation - Hashing	The application perform cryptographic hashing services not in accordance with FCS_COP.1.1(2) and uses the cryptographic algorithm RC2/RC4/MD4/MD5.
13	FCS_HTTPS_EXT.1.1	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement the HTTPS protocol that complies with RFC 2818.
14	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.
15	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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
16	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: ['RFC 5280 certificate validation and certificate path validation', 'The certificate path must terminate with a trusted CA certificate'].
17	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
api.cloud.appcelerator.com	good	**IP:** 35.167.69.72 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
www.w3.org	good	**IP:** 128.30.52.100 **Country:** United States of America **Region:** Massachusetts **City:** Cambridge **Latitude:** 42.365078 **Longitude:** -71.104523 **View:** Google Map
www.apparmor.com	good	**IP:** 104.45.152.13 **Country:** United States of America **Region:** Virginia **City:** Washington **Latitude:** 38.713451 **Longitude:** -78.159439 **View:** Google Map
apparmor.firebaseio.com	good	**IP:** 35.201.97.85 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
api.appcelerator.com	good	**IP:** 52.41.175.220 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
code.google.com	good	**IP:** 142.250.190.78 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
crbug.com	good	**IP:** 216.239.32.29 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

URLS

URL	FILE
https://api.appcelerator.com/p/v4/mobile-track	com/appcelerator/aps/APSAnalyticsMeta.java
file:///sdcard/	com/appcelerator/aps/APSCloudPush.java
https://api.cloud.appcelerator.com/v1	com/appcelerator/aps/PushConstants.java
http://www.apparmor.com	com/cutcom/apparmor/rit/TigersafeAppInfo.java
file:///android_asset/ file:///android_asset/Resources/	org/appcelerator/titanium/TiC.java
file:///android_asset/	org/appcelerator/titanium/TiLaunchActivity.java
file:///android_asset/	org/appcelerator/titanium/io/TiFileProvider.java
data://	org/appcelerator/titanium/io/TiFileFactory.java
file:///android_asset/	org/appcelerator/titanium/util/TiConvert.java
file:///android_asset/Resources	org/appcelerator/titanium/util/TiFileHelper.java
http://www.w3.org/XML/1998/namespace	org/jaxen/ContextSupport.java
http://www.w3.org/2000/xmlns/ http://www.w3.org/XML/1998/namespace	org/jaxen/dom/DocumentNavigator.java
http://www.w3.org/XML/1998/namespace	org/jaxen/function/LangFunction.java
file:///android_asset/	ti/modules/titanium/android/TiBroadcastReceiver.java
file:///android_asset/	ti/modules/titanium/android/TiJSService.java
file:///android_asset/	ti/modules/titanium/android/TiJSIntervalService.java
data://	ti/modules/titanium/filesystem/FilesystemModule.java

URL	FILE
https://api.appcelerator.com/p/v1/geo?	ti/modules/titanium/geolocation/TiLocation.java
https://apparmor.firebaseio.com http://code.google.com/p/zxing	Android String Resource
https://crbug.com/v8/8520	lib/arm64-v8a/libkroll-v8.so
https://crbug.com/v8/8520	lib/armeabi-v7a/libkroll-v8.so

FIREBASE DATABASES

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

EMAILS

EMAIL	FILE
jordi@iamyellow.net	com/cutcom/apparmor/rit/TigersafeApplication.java

TRACKERS

TRACKER	CATEGORIES	URL
Appcelerator Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/255
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

HARDCODED SECRETS

POSSIBLE SECRETS
"firebase_database_url" : "https://apparmor.firebaseio.com"
"google_api_key" : "AIzaSyDbBNTkdyMMRqLo4OKA3gigHDkUW9-y4Ow"
"google_crash_reporting_api_key" : "AIzaSyDbBNTkdyMMRqLo4OKA3gigHDkUW9-y4Ow"

PLAYSTORE INFORMATION

Title: Tigersafe - RIT

Score: 4.3333335 **Installs:** 1,000+ **Price:** 0 **Android Version Support:** 4.4 and up **Category:** Education **Play Store URL:** com.cutcom.apparmor.rit

Developer Details: Rochester Institute of Technology, Rochester+Institute+of+Technology, 1 Lomb Memorial Dr, Rochester, NY 14623, http://rit.edu, ritmobile@g.rit.edu,

Release Date: Oct 30, 2017 **Privacy Policy:** Privacy link

Description:

Tigersafe is the official safety app of Rochester Institute of Technology. It is the only app that integrates with RIT's safety and security systems. RIT Public Safety has worked to develop a unique app that provides students, faculty and staff with added safety on the RIT campus. The app will send you important safety alerts and provide instant access to campus safety resources. Tigersafe features include: - Mobile Bluelight: Send your location to RIT security in real-time in case of a crisis - Emergency Contacts: Contact the correct services for the RIT area in case of an emergency or a non-emergency concern - Tip Reporting: Multiple ways to report a safety/security concern directly to RIT Public Safety, or request assistance from Public Safety. - Friend Walk: Ask a friend to monitor your location as you walk home. - Safety notifications: Receive instant notifications and instructions from campus safety when on-campus emergencies occur. - Chat with Security: Communicate live with safety staff at RIT via chat. - Campus Map: Find your way around campus! - Campus safety resources: access all important safety resources in one convenient app. Download today and ensure that you're prepared in the event of an emergency.

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

Report Generated by - MobSF v3.4.5 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.