

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
1	App can be installed on a vulnerable unpatched Android versionAndroid 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.	Suppression the rule vulnerable_os_version in com.tange365.icam365
2	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.	Suppression the rule clear_text_traffic in com.tange365.icam365

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
3	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.	Suppression the rule has_network_security in com.tange365.icam365
4	Application Data can be Backed up[android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.	Suppression the rule app_allowbackup in com.tange365.icam365
5	Broadcast Receiver (com.taobao.accs.EventReceiver) is not Protected. [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.	Suppression the rule receiver_explicitly_exported in com.tange365.icam365
6	Activity (com.tg.app.activity.device.DeviceListActivity) 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.	Suppression the rule activity_explicitly_exported in com.tange365.icam365

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
7	Activity (com.tg.app.activity.CloudServiceActivity) 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.	Suppression the rule activity_explicitly_exported in com.tange365.icam365
8	Activity (com.tg.login.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.	Suppression the rule activity_explicitly_exported in com.tange365.icam365
9	Activity (com.tange365.icam365.wxapi.WXEntryActivity) 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.	Suppression the rule activity_explicitly_exported in com.tange365.icam365
10	Activity (com.tg.message.msg.MessagePlayActivity) 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.	Suppression the rule activity_explicitly_exported in com.tange365.icam365
11	Activity (com.tange365.pick.PickOrTakeImageActivity) 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.	Suppression the rule activity_explicitly_exported in com.tange365.icam365

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
12	Broadcast Receiver (com.tg.push.HmsMessageReceiver) is Protected by a permission, but the protection level of the permission should be checked.Permission: com.tange365.icam365.permission.HMS_RECEIVE [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.	Suppression the rule receiver_exported_protected_permission_not_defined in com.tange365.icam365
13	Service (com.vivo.push.sdk.service.CommandClientService) is not Protected. [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.	Suppression the rule service_explicitly_exported in com.tange365.icam365

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
14	Broadcast Receiver (com.tg.push.XiaoMiPushReceiver) is not Protected. [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.	Suppression the rule receiver_explicitly_exported in com.tange365.icam365
15	Service (com.xiaomi.mipush.sdk.PushMessageHandler) is Protected by a permission, but the protection level of the permission should be checked.Permission: com.xiaomi.xmsf.permission.MIPUSH_RECEIVE [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.	Suppression the rule service_exported_protected_permission_not_defined in com.tange365.icam365

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
16	Broadcast Receiver (com.xiaomi.push.service.receivers.NetworkStatusReceiver) is not Protected. [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.	Suppression the rule receiver_explicitly_exported in com.tange365.icam365
17	Service (com.tg.push.OppoAppPushMessageService) is Protected by a permission, but the protection level of the permission should be checked.Permission: com.coloros.mcs.permission.SEND_MCS_MESSAGE [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.	Suppression the rule service_exported_protected_permission_not_defined in com.tange365.icam365

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
18	Service (com.tg.push.OppoPushMessageService) is Protected by a permission, but the protection level of the permission should be checked.Permission: com.heytao.mcs.permission.SEND_PUSH_MESSAGE [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.	Suppression the rule service_exported_protected_permission_not_defined in com.tange365.icam365

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
19	Service (com.heytao.msp.push.service.CompatibleDataMessageCallbackService) is Protected by a permission, but the protection level of the permission should be checked.Permission: com.coloros.mcs.permission.SEND_MCS_MESSAGE [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.	Suppression the rule service_exported_protected_permission_not_defined in com.tange365.icam365



NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
20	Service (com.heytao.msp.push.service.DataMessageCallbackService) is Protected by a permission, but the protection level of the permission should be checked.Permission: com.heytao.mcs.permission.SEND_PUSH_MESSAGE [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.	Suppression the rule service_exported_protected_permission_not_defined in com.tange365.icam365
21	Activity (com.xiaomi.mipush.sdk.NotificationClickedActivity) 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.	Suppression the rule activity_explicitly_exported in com.tange365.icam365

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
22	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.	Suppression the rule receiver_exported_protected_permission_not_defined in com.tange365.icam365

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
23	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked.Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [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.	Suppression the rule service_exported_protected_permission_not_defined in com.tange365.icam365

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
24	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 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.	Suppression the rule receiver_exported_protected_permission_not_defined in com.tange365.icam365
25	Broadcast Receiver (com.huawei.hms.support.api.push.PushMsgReceiver) is Protected by a permission.Permission: com.tange365.icam365.permission.PROCESS_PUSH_MSGprotectionLevel: signature[android:exported=true]	info	A Broadcast Receiver is found to be exported, but is protected by permission.	Suppression the rule receiver_exported_protected_permission_signature in com.tange365.icam365
26	Broadcast Receiver (com.huawei.hms.support.api.push.PushReceiver) is Protected by a permission.Permission: com.tange365.icam365.permission.PROCESS_PUSH_MSGprotectionLevel: signature[android:exported=true]	info	A Broadcast Receiver is found to be exported, but is protected by permission.	Suppression the rule receiver_exported_protected_permission_signature in com.tange365.icam365

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
27	Service (com.huawei.hms.support.api.push.service.HmsMsgService) is not Protected. [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.	Suppression the rule service_explicitly_exported in com.tange365.icam365
28	Content Provider (com.huawei.hms.support.api.push.PushProvider) is not Protected. [android:exported=true]	warning	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.	Suppression the rule provider_explicitly_exported in com.tange365.icam365
29	Activity (com.bytedance.android.openliveplugin.stub.activity.DouyinAuthorizeActivityProxy) 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.	Suppression the rule activity_explicitly_exported in com.tange365.icam365
30	Activity (com.bytedance.android.openliveplugin.stub.activity.DouyinAuthorizeActivityLiveProcessProxy) 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.	Suppression the rule activity_explicitly_exported in com.tange365.icam365
31	Activity (com.alipay.sdk.app.PayResultActivity) 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.	Suppression the rule activity_explicitly_exported in com.tange365.icam365

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
32	Activity (com.alipay.sdk.app.AlipayResultActivity) 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.	Suppression the rule activity_explicitly_exported in com.tange365.icam365
33	Activity (com.mcto.spsdk.feedback.FeedBackActivity) 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.	Suppression the rule activity_explicitly_exported in com.tange365.icam365