



MIUI security components 1.3.8.APK 分析报告



APP名称:

MIUI security components

包名:	com.miui.guardprovider
域名线索:	10条
URL线索:	8条
邮箱线索:	1条
分析日期:	2024年4月19日
分析平台:	摸瓜反编译平台

文件信息

文件名: MIUIGuardProvider.apk

文件大小: 10.3MB
MD5值: 9592ca40e06ca93154e8e020462b7e44
SHA1值: 98a58ce7f9f6a913f0b8502798301b3f3d1e4945
SHA256值: 0f9d7dd97a45a37489da30b5e4c70cbd0483f5585c6eefbadba131834b5be1c8

i APP 信息

App名称: MIUI security components
包名: com.miui.guardprovider
主活动Activity:
安卓版本名称: 1.3.8
安卓版本: 138

🔍 域名线索

域名	服务器信息
mmgr.gting.com	IP: 221.204.165.203 所属国家: China 地区: Shanxi 城市: Taiyuan 纬度: 37.869438 经度: 112.561508
tmfsdk.m.qq.com	IP: 175.27.12.246 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
tmfsdk4.m.qq.com	IP: 175.27.12.246 所属国家: China 地区: Beijing 城市: Beijing

	纬度: 39.907501 经度: 116.397102
miwifi.com	IP: 183.84.5.58 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
log.avlyun.sec.intl.miui.com	没有服务器地理信息.
tools.3g.qq.com	IP: 109.244.244.106 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
staging.api.sec.miui.com	没有服务器地理信息.
m.qq.com	IP: 109.244.244.106 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
api.sec.miui.com	IP: 183.84.7.86 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
api.sec.intl.miui.com	IP: 8.219.247.14 所属国家: Singapore 地区: Singapore 城市: Singapore

纬度: 1.289987
经度: 103.850281

 URL线索

URL信息	Url所在文件
https://mmgr.gting.com/qqsecure_config_update/qqsecure_config_update][UpdateManager]	tmsdk/common/module/update/a.java
https://tools.3g.qq.com/wifi/cw.html	tmsdkobf/mg.java
http://tools.3g.qq.com/wifi/cw.html]customHeader:[Meri]	tmsdkobf/jf.java
http://tools.3g.qq.com/wifi/cw.html	tmsdkobf/jf.java
http://miwifi.com/diagnosis/index.html	tmsdkobf/jf.java
http://tools.3g.qq.com/j/sslstrip	tmsdkobf/jf.java
http://m.qq.com	tmsdkobf/jf.java
https://tmfsdk.m.qq.com	tmsdkobf/xa.java
https://tmfsdk4.m.qq.com	tmsdkobf/xa.java
https://log.avlyun.sec.intl.miui.com/logupload	com/miui/guardprovider/engine/antiy/AvlEngine.java
https://api.sec.miui.com/antivirus/viruses	com/miui/guardprovider/engine/mi/antivirus/tools/AntivirusImpl.java
https://api.sec.intl.miui.com/antivirus/viruses	com/miui/guardprovider/engine/mi/antivirus/tools/AntivirusImpl.java
http://staging.api.sec.miui.com/antivirus/viruses	com/miui/guardprovider/engine/mi/antivirus/tools/AntivirusImpl.java

http://api.sec.miui.com/policy/proxy?p=avast&l=en_US	Mogua Engine V1
http://api.sec.miui.com/policy/proxy?p=antiy&l=en_US	Mogua Engine V1
http://api.sec.miui.com/policy/proxy?p=tencent&l=en_US	Mogua Engine V1
http://api.sec.miui.com/policy/proxy?p=avast&l=en_US	Mogua Engine V1
http://api.sec.miui.com/policy/proxy?p=avast&l=zh_TW	Mogua Engine V1
http://api.sec.miui.com/policy/proxy?p=antiy&l=zh_TW	Mogua Engine V1
http://api.sec.miui.com/policy/proxy?p=tencent&l=zh_TW	Mogua Engine V1
http://api.sec.miui.com/policy/proxy?p=avast&l=zh_CN	Mogua Engine V1
http://api.sec.miui.com/policy/proxy?p=antiy&l=zh_CN	Mogua Engine V1
http://api.sec.miui.com/policy/proxy?p=tencent&l=zh_CN	Mogua Engine V1
http://api.sec.miui.com/policy/proxy?p=avastl=en_US	Mogua Engine V1

 邮箱线索

邮箱地址	所在文件
.apk@classes.dex	com/tencent/turingfd/sdk/vd/j0.java

 手机线索

手机号	所在文件
17179869184	tmsdk/common/module/update/UpdateConfig.java

🌸 签名证书

APK已签名
v1 签名: True
v2 签名: True
v3 签名: True
找到 1 个唯一证书
主题: C=CN, ST=Beijing, L=Beijing, O=Xiaomi, OU=MIUI, CN=MIUI, E=miui@xiaomi.com
签名算法: rsassa_pkcs1v15
有效期自: 2011-12-06 03:26:26+00:00
有效期至: 2039-04-23 03:26:26+00:00
发行人: C=CN, ST=Beijing, L=Beijing, O=Xiaomi, OU=MIUI, CN=MIUI, E=miui@xiaomi.com
序列号: 0xe552a8ecb9011b7c
哈希算法: sha1
md5值: 701478a1e3b4b7e3978ea69469410f13
sha1值: 7b6dc7079c34739ce81159719fb5eb61d2a03225
sha256值: c9009d01ebf9f5d0302bc71b2fe9aa9a47a432bba17308a3111b75d7b2149025
sha512值: 83bcc6127662a62784e99c81038073d3493153c87417d413c0f2cbf9d9d15709e0234149589883deb08426c210fd52b4eb848d771cea8209e79c0a93f0b23cf4
公钥算法: rsa
密钥长度: 2048
指纹: a5cbecd2fbc7fe481cc5137b011d3b095eb9f94145eb43571524d1a7d80466b4

🔑 硬编码敏感信息

🔗 加壳分析

🏢 第三方SDK

☰ 此APP的危险动作

向手机申请的权限	是否危险	类型	详细情况
android.permission.READ_PHONE_STATE	危险	读取电话状态和身份	允许应用访问设备的电话功能。具有此权限的应用程序可以确定此电话的电话号码和序列号,呼叫是否处于活动状态,呼叫所连接的号码等
android.permission.READ_PRIVILEGED_PHONE_STATE	未知	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_NETWORK_STATE	正常	查看网络状态	允许应用程序查看所有网络的状态
android.permission.CHANGE_NETWORK_STATE	正常	更改网络连接	允许应用程序更改网络连接状态。
android.permission.ACCESS_WIFI_STATE	正常	查看Wi-Fi状态	允许应用程序查看有关 Wi-Fi 状态的信息
android.permission.CHANGE_WIFI_STATE	正常	更改Wi-Fi状态	允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改
android.permission.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
android.permission.READ_EXTERNAL_STORAGE	危险	读取外部存储器内容	允许应用程序从外部存储读取
android.permission.WRITE_EXTERNAL_STORAGE	危险	读取/修改/删除外部存储内容	允许应用程序写入外部存储

android.permission.ACCESS_COARSE_LOCATION	危险	粗定位	访问粗略位置源,例如移动网络数据库,以确定大概的电话位置（如果可用）。恶意应用程序可以使用它来确定您的大致位置
android.permission.PEERS_MAC_ADDRESS	未知	Unknown permission	Unknown permission from android reference
com.miui.securitycenter.permission.ACCESS_SECURITY_CENTER_PROVIDER	未知	Unknown permission	Unknown permission from android reference
android.permission.RECEIVE_BOOT_COMPLETED	正常	开机时自动启动	允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度
com.android.settings.permission.CLOUD_SETTINGS_PROVIDER	未知	Unknown permission	Unknown permission from android reference
android.permission.INTERACT_ACROSS_USERS	未知	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_MTP	未知	Unknown permission	Unknown permission from android reference
android.permission.MANAGE_EXTERNAL_STORAGE	危险	允许应用程序广泛访问范围存储中的外部存储	允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用
com.miui.guardprovider.permission.Guard_Provider	未知	Unknown permission	Unknown permission from android reference
android.permission.QUERY_ALL_PACKAGES	正常		允许查询设备上的任何普通应用程序,无论清单声明如何
android.permission.WAKE_LOCK	正常	防止手机睡眠	允许应用程序防止手机进入睡眠状态
android.permission.READ_APN_SETTINGS	未知	Unknown permission	Unknown permission from android reference

android.permission.BROADCAST_STICKY	正常	发送粘性广播	允许应用程序发送粘性广播,在广播结束后保留。恶意应用程序会导致手机使用过多内存,从而使手机运行缓慢或不稳定
android.permission.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。
com.miui.guardprovider.permission.TMF_SHARK	未知	Unknown permission	Unknown permission from android reference

应用内通信

报告由 [摸瓜APK反编译平台](#) 自动生成，并非包含所有检测结果，有疑问请联系管理员。