Evaluation Warning: The document was created with Spire.Doc for Python.

**MIUI security components（ 1.4.3版本）
APK分析报告**

## **1. 分析结果概述**

**说明：本分析结果由摸瓜网站自动生成，一共包含以下10类内容：（1）分析结果概述（2）APK文件基本信息（3）APP基本信息（4）线索情况（5）签名证书（6）硬编码敏感信息（7）加壳分析（8）第三方插件（9）此APP的危险动作（10）应用内通信。
\*此分析结果仅供参考，请勿商用。\*。**

| 类别 | 内容 |
| --- | --- |
| APP名称 | MIUI security components |
| 版本 | 1.4.3 |
| 包名 | com.miui.guardprovider |
| 域名线索 | 16条 |
| URL线索 | 11条 |
| APP图标 |  |
| 分析日期 | 2025年5月9日 |
| 分析平台 | [摸瓜APK反编译平台](https://mogua.co) |

## **2. APK文件基本信息**

| 类别 | 内容 |
| --- | --- |
| 文件名 | MIUIGuardProvider.apk |
| 文件大小 | 8.62MB |
| MD5值 | baf42d5a0e84f7904b82a0320298b833 |
| SHA1值 | 4a6868350bef9340db4db3fad38d10acb0b07b3a |
| SHA256值 | 3dae9342ede08a4b69e51820f762b646b8da3577092e81a82f3f1c39d092b19a |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | MIUI security components |
| 包名 | com.miui.guardprovider |
| 主活动Activity |  |
| 安卓版本名称 | 1.4.3 |
| 安卓版本 | 143 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| www.baidu.com | IP: 110.242.68.4 所属国家: China 地区: Hebei 城市: Baoding  |
| log.avlyun.sec.intl.miui.com | IP: 159.138.235.168 所属国家: Thailand 地区: Krung Thep Maha Nakhon 城市: Bangkok  |
| api.sec.miui.com | IP: 183.84.6.87 所属国家: China 地区: Beijing 城市: Beijing  |
| tools.3g.qq.com | IP: 109.244.244.106 所属国家: China 地区: Beijing 城市: Beijing  |
| staging.api.sec.miui.com | 没有服务器地理信息.  |
| tmfsdk.m.qq.com | IP: 175.27.12.246 所属国家: China 地区: Beijing 城市: Beijing  |
| www.w3.org | IP: 128.30.52.100 所属国家: United States of America 地区: Massachusetts 城市: Cambridge  |
| www.qq.com | IP: 175.27.8.138 所属国家: China 地区: Beijing 城市: Beijing  |
| flash.sec.miui.com | IP: 183.84.5.170 所属国家: China 地区: Beijing 城市: Beijing  |
| www.openssl.org | IP: 23.2.129.55 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| www.ro | IP: 193.230.31.206 所属国家: Romania 地区: Bucuresti 城市: Bucharest  |
| mmgr.gtimg.com | IP: 182.254.54.197 所属国家: China 地区: Guangdong 城市: Shenzhen  |
| tmfsdk4.m.qq.com | IP: 175.27.12.246 所属国家: China 地区: Beijing 城市: Beijing  |
| m.qq.com | IP: 109.244.244.78 所属国家: China 地区: Beijing 城市: Beijing  |
| www.wapforum.org | IP: 172.67.190.29 所属国家: United States of America 地区: California 城市: San Francisco  |
| miwifi.com | IP: 183.84.5.58 所属国家: China 地区: Beijing 城市: Beijing  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://api.sec.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  |
| https://api.sec.miui.com/antivirus/whitelist  | com/miui/guardprovider/engine/mi/antivirus/tools/AntivirusImpl.java  |
| http://staging.api.sec.miui.com/antivirus/whitelist  | com/miui/guardprovider/engine/mi/antivirus/tools/AntivirusImpl.java  |
| https://flash.sec.miui.com/detect/app  | com/miui/guardprovider/engine/mi/antidefraud/AntiDefraudAppManager.java  |
| https://log.avlyun.sec.intl.miui.com/logupload  | com/miui/guardprovider/engine/antiy/AvlEngine.java  |
| https://mmgr.gtimg.com/qqsecure\_config\_update/qqsecure\_config\_update  | tmsdk/common/module/update/a.java  |
| http://tools.3g.qq.com/wifi/cw.html  | tmsdkobf/p9.java  |
| http://miwifi.com/diagnosis/index.html  | tmsdkobf/p9.java  |
| http://tools.3g.qq.com/j/sslstrip  | tmsdkobf/p9.java  |
| http://m.qq.com  | tmsdkobf/p9.java  |
| https://tmfsdk.m.qq.com  | tmsdkobf/w5.java  |
| https://tmfsdk4.m.qq.com  | tmsdkobf/w5.java  |
| www.qq.com  | tmsdkobf/m8.java  |
| http://api.sec.miui.com/policy/proxy?p=avast&l=en\_US  | Android String Resource  |
| http://api.sec.miui.com/policy/proxy?p=antiy&l=en\_US  | Android String Resource  |
| http://api.sec.miui.com/policy/proxy?p=tencent&l=en\_US  | Android String Resource  |
| http://api.sec.miui.com/policy/proxy?p=avast&amp;l=en\_US  | Android String Resource  |
| http://api.sec.miui.com/policy/proxy?p=avast&l=zh\_TW  | Android String Resource  |
| http://api.sec.miui.com/policy/proxy?p=antiy&l=zh\_TW  | Android String Resource  |
| http://api.sec.miui.com/policy/proxy?p=tencent&l=zh\_TW  | Android String Resource  |
| http://api.sec.miui.com/policy/proxy?p=avast&l=zh\_CN  | Android String Resource  |
| http://api.sec.miui.com/policy/proxy?p=antiy&l=zh\_CN  | Android String Resource  |
| http://api.sec.miui.com/policy/proxy?p=tencent&l=zh\_CN  | Android String Resource  |
| http://api.sec.miui.com/policy/proxy?p=avastl=en\_US  | Android String Resource  |
| www.ro  | lib/arm64-v8a/libavlurl.so  |
| http://%s  | lib/arm64-v8a/libavlurl.so  |
| www.baidu.com  | lib/arm64-v8a/libavlm.so  |
| http://www.wapforum.org  | lib/arm64-v8a/libavlm.so  |
| http://www.w3.org  | lib/arm64-v8a/libavlm.so  |
| http://www.openssl.org/support/faq.html  | lib/arm64-v8a/libavlm.so  |

### **4.3 邮箱线索**

### **4.4 手机号线索**

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

## **5. 签名证书**

**APK is signed v1 signature: True v2 signature: True v3 signature: True Found 1 unique certificates Subject: C=CN, ST=Beijing, L=Beijing, O=Xiaomi, OU=MIUI, CN=MIUI, E=miui@xiaomi.com Signature Algorithm: rsassa\_pkcs1v15 Valid From: 2011-12-06 03:26:26+00:00 Valid To: 2039-04-23 03:26:26+00:00 Issuer: C=CN, ST=Beijing, L=Beijing, O=Xiaomi, OU=MIUI, CN=MIUI, E=miui@xiaomi.com Serial Number: 0xe552a8ecb9011b7c Hash Algorithm: sha1 md5: 701478a1e3b4b7e3978ea69469410f13 sha1: 7b6dc7079c34739ce81159719fb5eb61d2a03225 sha256: c9009d01ebf9f5d0302bc71b2fe9aa9a47a432bba17308a3111b75d7b2149025 sha512: 83bcc6127662a62784e99c81038073d3493153c87417d413c0f2cbf9d9d15709e0234149589883deb08426c210fd52b4eb848d771cea8209e79c0a93f0b23cf4 PublicKey Algorithm: rsa Bit Size: 2048 Fingerprint: a5cbecd2fbc7fe481cc5137b011d3b095eb9f94145eb43571524d1a7d80466b4**

## **6. 硬编码敏感信息**

## **7. 加壳分析**

| 加壳类型 | 所属文件 |
| --- | --- |
| 登陆摸瓜网站后查看  |  |

## **8. 第三方插件**

| 名称 | 分类 | URL链接 |
| --- | --- | --- |
| 登陆摸瓜网站后查看  |  |  |

## **9. 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 |
| 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 |
| com.miui.guardprovider.permission.Guard\_Provider | 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 |
| com.miui.guardprovider.permission.TMF\_SHARK | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

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