南明离火
移动应用检测平台

ANDROID 静态分析报告

MobileWips • v1.2.01.17

分析日期: 2025-03-10 23:49:22

应用概览

文件名称:	6ff03c3f265ac92b326031d5a45f2be3b5a60a4b49e23e1dc75ee1312ac30bda.apk
文件大小:	3.72MB
应用名称:	MobileWips
软件包名:	com.samsung.android.server.wifi.mobilewips
主活动:	not_found_main_activity!!
版本号:	1.2.01.17
最小SDK:	28
目标SDK:	33
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	52/100 (中风险)
杀软检测:	AI评估：安全
MD5:	20ce87d643edeee7d278c3de5ac625d6
SHA1:	edaa4260a56f0e656a07e92bcd6490abfae671e0
SHA256:	6ff03c3f265ac92b326031d5a45f2be3b5a60a4b49e23e1dc75ee1312ac30bda

分析结果严重性

高危	中危	信息	安全	关注
1	3	1	1	1

四大组件信息

Activity组件：0个，其中export的有：0个
Service组件：1个，其中export的有：0个
Receiver组件：0个，其中export的有：0个
Provider组件：1个，其中export的有：1个

证书信息

二进制文件已签名
v1 签名: False
v2 签名: False

v3 签名: True
v4 签名: False
主题: C=KR, ST=South Korea, L=Suwon City, O=Samsung Corporation, OU=DMC, CN=Samsung Cert, E=android.os@samsung.com
签名算法: rsassa_pkcs1v15
有效期自: 2011-06-22 12:25:12+00:00
有效期至: 2038-11-07 12:25:12+00:00
发行人: C=KR, ST=South Korea, L=Suwon City, O=Samsung Corporation, OU=DMC, CN=Samsung Cert, E=android.os@samsung.com
序列号: 0xd20995a79c0daad6
哈希算法: sha1
证书MD5: d087e72912fba064cafa78dc34aea839
证书SHA1: 9ca5170f381919dfe0446fcdab18b19a143b3163
证书SHA256: 34df0e7a9f1cf1892e45c056b4973cd81ccf148a4050d11aea4ac5a65f900a42
证书SHA512:
0018b67dbb7cbe4ce3ed227c683e63738c491530c59ed76432b6172f78adb2fa98d50230f9d668cdda29e6b80a3718dbad001de679ed0[illegible]6a6037dc3ce0ed5782

公钥算法: rsa
密钥长度: 2048
指纹: 4cc6504a733cc2d6660a290b24312cc9f58cb95a4783747057d2796260379902
找到 1 个唯一证书

应用权限

权限名称	安全等级	权限内容	权限描述
android.Manifest.permission.KNOX_DEVICE_CONFIGURATION	未知	未知权限	来自 android 引用的未知权限。
android.permission.ACCESS_FINE_LOCATION	未知	未知权限	来自 android 引用的未知权限。
android.permission.ACCESS_NETWORK_STATE	普通	获取网络状态	允许应用程序查看所有网络的状态。
android.permission.ACCESS_WIFI_STATE	普通	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.INTERACT_ACROSS_USERS	未知	未知权限	来自 android 引用的未知权限。
android.permission.INTERNET	危险	完全互联网访问	允许应用程序创建网络套接字。
android.permission.LOCAL_MAC_ADDRESS	未知	未知权限	来自 android 引用的未知权限。
android.permission.SYSTEM_ALERT_WINDOW	危险	弹窗	允许应用程序弹窗。 恶意程序可以接管手机的整个屏幕。
com.samsung.permission.WIFI_WIPS	未知	未知权限	来自 android 引用的未知权限。

网络通信安全

序号	范围	严重级别	描述

证书安全分析

高危: 0 | 警告: 0 | 信息: 1

标题	严重程度	描述信息
已签名应用	信息	应用程序使用代码签名证书进行签名

MANIFEST分析

高危: **0** | 警告: **2** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用程序已启用明文网络流量 [android:usesCleartextTraffic=true]	警告	应用程序打算使用明文网络流量，例如明文HTTP，FTP协议，DownloadManager和MediaPlayer。针对API级别27或更低的应用程序，默认值为“true”。针对API级别28或更高的应用程序，默认值为“false”。避免使用明文流量的主要原因是缺乏机密性，真实性和防篡改保护；网络攻击者可以窃听传输的数据，并且可以在不被检测到的情况下修改它。
2	Content Provider (com.samsung.android.server.wifi.mobilewips.SemMobileWipsProvider) 受权限保护, 但是应该检查权限的保护级别。 Permission: com.samsung.permission.WIFI_WIPS [android:exported=true]	警告	发现一个 Content Provider被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。

</> 安全漏洞检测

高危: **1** | 警告: **5** | 信息: **1** | 安全: **0** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	应用程序记录日志信息,不得记录敏感信息	信息	CWE: CWE-532: 通过日志文件的信息暴露 OWASP MASVS: MSTG-STORAGE-3	升级会员：解锁高级权限
2	应用程序可以读取/写入外部存储器，任何应用程序都可以读取写入外部存储器的数据	警告	CWE: CWE-276: 默认权限不正确 OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	升级会员：解锁高级权限
3	应用程序在加密算法中使用ECB模式。ECB模式是已知的弱模式，因为它对相同的明文块[UNK]产生相同的密文	高危	CWE: CWE-327: 使用已破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-2	升级会员：解锁高级权限
4	IP地址泄露	警告	CWE: CWE-200: 信息泄露 OWASP MASVS: MSTG-CODE-2	升级会员：解锁高级权限
5	应用程序使用不安全的随机数生成器	警告	CWE: CWE-330: 使用不充分的随机数 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	升级会员：解锁高级权限

6	文件可能包含硬编码的敏感信息，如用户名、密码、密钥等	警告	CWE: CWE-312: 明文存储敏感信息 OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	升级会员：解锁高级权限
7	应用程序使用SQLite数据库并执行原始SQL查询。原始SQL查询中不受信任的用户输入可能会导致SQL注入。敏感信息也应加密并写入数据库	警告	CWE: CWE-89: SQL命令中使用的特殊元素转义处理不恰当（'SQL 注入'） OWASP Top 10: M7: Client Code Quality	升级会员：解锁高级权限

行为分析

编号	行为	标签	文件
00013	读取文件并将其放入流中	文件	升级会员：解锁高级权限
00022	从给定的文件绝对路径打开文件	文件	升级会员：解锁高级权限
00096	连接到 URL 并设置请求方法	命令 网络	升级会员：解锁高级权限
00089	连接到 URL 并接收来自服务器的输入流	命令 网络	升级会员：解锁高级权限
00030	通过给定的 URL 连接到远程服务器	网络	升级会员：解锁高级权限
00109	连接到 URL 并获取响应代码	网络 命令	升级会员：解锁高级权限
00052	删除内容 URI 指定的媒体（SMS、CALL_LOG、文件等）	短信	升级会员：解锁高级权限
00011	从 URI 查询数据（SMS、CALLLOGS）	短信 通话记录 信息收集	升级会员：解锁高级权限
00187	查询 URI 并检查结果	信息收集 短信 通话记录 日历	升级会员：解锁高级权限
00077	读取敏感数据（短信、通话记录等）	信息收集 短信 通话记录 日历	升级会员：解锁高级权限

敏感权限分析

类型	匹配	权限
恶意软件常用权限	1/30	android.permission.SYSTEM_ALERT_WINDOW
其它常用权限	3/46	android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.INTERNET

常用: 已知恶意软件广泛滥用的权限。

其它常用权限: 已知恶意软件经常滥用的权限。

域名检测

域名	状态	中国境内	位置信息
www.wordpress.org	安全	否	**IP地址:** 198.143.164.252 **国家:** 美国 **地区:** 伊利诺伊州 **城市:** 芝加哥 **纬度:** 41.875771 **经度:** -87.620655 **查看:** Google 地图
www.craigslist.org	安全	否	**IP地址:** 208.82.238.241 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.792030 **经度:** -122.406833 **查看:** Google 地图
www.ecosia.org	安全	否	**IP地址:** 104.18.37.185 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
www.ietf.org	安全	否	**IP地址:** 104.16.45.99 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
www.rsc.org	安全	否	**IP地址:** 104.18.37.185 **国家:** 大不列颠及北爱尔兰联合王国 **地区:** 苏格兰 **城市:** 格拉斯哥港 **纬度:** 55.934639 **经度:** -4.689500 **查看:** Google 地图
www.ieee.org	安全	否	**IP地址:** 108.139.10.103 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.774929 **经度:** -122.419418 **查看:** Google 地图
www.dmv.org	安全	否	**IP地址:** 13.249.126.115 **国家:** 美国 **地区:** 佐治亚州 **城市:** 亚特兰大 **纬度:** 33.748795 **经度:** -84.387543 **查看:** Google 地图

www.collegeboard.org	安全	否	**IP地址:** 104.17.88.51 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 洛杉矶 **纬度:** 34.052570 **经度:** -118.243904 **查看:** Google 地图
www.rfa.org	安全	否	**IP地址:** 23.45.40.192 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 洛杉矶 **纬度:** 34.052570 **经度:** -118.243904 **查看:** Google 地图
www.kernel.org	安全	否	**IP地址:** 151.101.129.55 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
www.tizen.org	安全	否	**IP地址:** 61.147.219.216 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 洛杉矶 **纬度:** 34.052570 **经度:** -118.243904 **查看:** Google 地图
www.acs.org	安全	否	**IP地址:** 104.18.37.185 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
www.python.org	安全	否	**IP地址:** 151.101.129.55 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
www.wikisource.org	安全	否	**IP地址:** 198.35.26.96 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.791256 **经度:** -122.400810 **查看:** Google 地图
www.mozilla.org	安全	否	**IP地址:** 104.18.37.185 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图

www.change.org	安全	否	**IP地址:** 151.101.129.55 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
www.jstor.org	安全	否	**IP地址:** 151.101.0.152 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
www.samsungsds.com	安全	否	**IP地址:** 45.223.136.179 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 红木城 **纬度:** 37.532440 **经度:** -122.248833 **查看:** Google 地图
www.code.org	安全	否	**IP地址:** 3.163.125.35 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 洛杉矶 **纬度:** 34.052570 **经度:** -118.243904 **查看:** Google 地图
www.cambridge.org	安全	否	**IP地址:** 104.17.111.190 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
www.npr.org	安全	否	**IP地址:** 23.206.229.209 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 洛杉矶 **纬度:** 34.052570 **经度:** -118.243904 **查看:** Google 地图
www.semanticscholar.org	安全	否	**IP地址:** 13.226.255.126 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 洛杉矶 **纬度:** 34.052570 **经度:** -118.243904 **查看:** Google 地图
www.android.com	安全	否	**IP地址:** 142.250.217.142 **国家:** 美国 **地区:** 佛罗里达州 **城市:** 迈阿密 **纬度:** 25.774269 **经度:** -80.193604 **查看:** Google 地图

www.acm.org	安全	否	**IP地址:** 104.17.79.30 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
www.samsung.com	安全	是	**IP地址:** 61.147.219.216 **国家:** 中国 **地区:** 江苏 **城市:** 南通 **纬度:** 32.030296 **经度:** 120.874779 **查看:** 高德地图
www.sciencemag.org	安全	否	**IP地址:** 172.64.146.13 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
www.samsungknox.com	安全	否	**IP地址:** 23.206.229.209 **国家:** 爱尔兰 **地区:** 都柏林 **城市:** 都柏林 **纬度:** 53.344151 **经度:** -6.267249 **查看:** Google 地图
www.hltv.org	安全	否	**IP地址:** 172.64.146.44 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图

URL链接分析

URL信息	源码文件
• 239.255.255.250 • 224.0.0.251	com/samsung/android/server/wifi/mobilewips/b/c.java

• http://www.android.com • http://www.python.org • http://www.mozilla.org • http://www.ieee.org • http://www.collegeboard.org • http://www.samsungsds.com • http://www.rfa.org • http://www.sciencemag.org • http://www.kernel.org • http://www.semanticscholar.org • http://www.wordpress.org • http://www.acm.org • http://www.craigslist.org • http://www.samsungknox.com • http://www.dmv.org • http://www.wikisource.org • http://www.samsung.com • http://www.code.org • http://www.ecosia.org • http://www.jstor.org • http://www.acs.org • http://www.rsc.org • http://www.hltv.org • http://www.change.org • http://www.npr.org • http://www.ietf.org • http://www.cambridge.org • http://www.tizen.org	com/samsung/android/server/wifi/mobilewips/d/m.java
• 216.58.202.4 • www.google.com	com/samsung/android/server/wifi/mobilewips/d/e.java

第三方SDK

SDK名称	开发者	描述信息
Conscrypt	Google	Conscrypt 是一个 Java 安全提供程序 (JSP)，它实现了部分 Java 加密扩展 (JCE) 和 Java 安全套接字扩展 (JSSE)。 它使用 BoringSSL 为 Android 和 OpenJDK 上的 Java 应用程序提供加密原语和传输层安全性 (TLS)。 有关所提供内容的详细信息，请参阅功能文档。

密钥凭证

可能的密钥
gD63hSj3ScS+wdCveGxxbXlq35N1c5Lby/S4T7MITjxo=
etPaaIxcBWY1cUeGpwvPMCJMwlRVNxv1fkIYtktoJTQ=
a3785913ca4deb75abd841414a0a700098e879777940c78c73fe6f2bee6c0352
AW5uAoTSTDfG5NfY1bp08GUnOqlRb+HVhbJ3ODJvsE=
b0a00e4a271beec4fee42fad0618432fa7d7fb3d99004d2b0bdfc14f8024832b

免责声明及风险提示:

本报告由南明离火移动安全分析平台自动生成，内容仅供参考，不构成任何法律意见或建议。本平台对使用本产品及其内容所引发的任何直接或间接损