南明离火
移动应用检测平台

ANDROID 静态分析报告

MIUI 主题工具 • v2.6.2

分析日期: 2024-05-26 13:27:06

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

应用概览

文件名称:	MIUI_killer.apk
文件大小:	3.49MB
应用名称:	MIUI 主题工具
软件包名:	org.hydev.new.themeapplytools
主活动:	org.hydev.themeapplytools.activity.MainActivity
版本号:	2.6.2
最小SDK:	24
目标SDK:	30
加固信息:	未加壳
应用程序安全分数:	55/100 (中风险)
杀软检测:	AI评估：安全
MD5:	30d53fc69d32406c809eef1e2f501258
SHA1:	56ba357a4e76a843462e9e91d938e13b29dbf673
SHA256:	2e4f17f866ecc2debfba9281c978b5f1966a411a17a0b3b9fa6252cecb4e80aa

分析结果严重性分布

高危	中危	信息	安全	关注
1	2	2	1	0

四大组件导出状态统计

Activity组件：7个，其中export的有：0个
Service组件：0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：0个

应用签名证书信息

二进制文件已签名
v1 签名: True
v2 签名: False
v3 签名: False

本报告由南明离火移动安全分析平台生成

v4 签名: False
主题: C=cn, ST=ak, L=ak, O=androidkiller, OU=androidkiller, CN=androidkiller
签名算法: rsassa_pkcs1v15
有效期自: 2014-12-23 06:27:44+00:00
有效期至: 2069-09-25 06:27:44+00:00
发行人: C=cn, ST=ak, L=ak, O=androidkiller, OU=androidkiller, CN=androidkiller
序列号: 0x661d0629
哈希算法: sha256
证书MD5: 6230025aa9d683803c2bec499f6be89b
证书SHA1: ac4c35dbb80e320ac5e432f4991fd81798191c68
证书SHA256: 927d5aa90736d7b8d1b1f06978bb3697395caf14f794544158f37abd0f21df6d
证书SHA512:
50a756bf495b76d7583b0d1970eb4bfd7b7a7f4754bd57f486a2ba9996b7ccb8a4f88fdcf16189634909819b2b35e81654a4f687b59177[illegible]cb3bdf27036a

找到 1 个唯一证书

权限声明与风险分级

权限名称	安全等级	权限内容	权限描述
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.READ_EXTERNAL_STORAGE	危险	读取SD卡内容	允许应用程序从SD卡读取信息。

网络通信安全风险分析

序号	范围	严重级别	描述

证书安全合规分析

高危: **1** | 警告: **0** | 信息: **1**

标题	严重程度	描述信息
已签名应用	信息	应用程序已使用代码签名证书进行签名
应用程序存在Janus漏洞	高危	应用程序使用了v1签名方案进行签名，如果只使用v1签名方案，那么它就容易受到安卓5.0-8.0上的Janus漏洞的攻击。在安卓5.0-7.0上运行的使用了v1签名方案的应用程序，以及同时使用了v2/v3签名方案的应用程序也同样存在漏洞。

Manifest 配置安全分析

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

序号	问题	严重程度	描述信息
1	应用程序可以安装在有漏洞的已更新 Android 版本上 Android 7.0, [minSdk=24]	信息	该应用程序可以安装在具有多个未修复漏洞的旧版本 Android 上。这些设备不会从 Google 接收合理的安全更新。支持 Android 版本 => 10、API 29 以接收合理的安全更新。
2	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。

本报告由南明离火移动安全分析平台生成

代码安全漏洞检测

高危: **0** | 警告: **1** | 信息: **2** | 安全: **0** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	应用程序可以写入应用程序目录。敏感信息应加密	信息	CWE: CWE-276: 默认权限不正确 OWASP MASVS: MSTG-STORAGE-14	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	此应用程序将数据复制到剪贴板。敏感数据不应复制到剪贴板，因为其他应用程序可以访问它	信息	OWASP MASVS: MSTG-STORAGE-10	升级会员：解锁高级权限

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	0/30	
其它常用权限	2/46	android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE

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。

第三方 SDK 组件分析

SDK名称	开发者	描述信息
File Provider	Android	FileProvider 是 ContentProvider 的特殊子类，它通过创建 content://Uri 代替 file:///Uri 以促进安全分享与应用程序关联的文件。

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失概不负责。本报告内容仅供网络安全研究，不得违反中华人民共和国相关法律法规。如有任何疑问，请及时与我们联系。

南明离火移动安全分析平台是一款专业的移动端恶意软件分析和安全评估框架。它能够执行静态分析和动态分析，深入扫描软件中中潜在的漏洞和安全隐隐患。

© 2025 南明离火 - 移动安全分析平台自动生成

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成