南明离火
移动应用检测平台

ANDROID 静态分析报告

XT工具箱 • v3.6.15

分析日期: 2025-10-07 02:00:42

应用概览

文件名称:	XT工具箱_3.6.15.Apk
文件大小:	42.09MB
应用名称:	XT工具箱
软件包名:	xiaote.tool
主活动:	net.fusionapp.core.WelcomeActivity
版本号:	3.6.15
最小SDK:	23
目标SDK:	29
加固信息:	未加壳
开发框架:	LuaJava
应用程序安全分数:	32/100 (高风险)
杀软检测:	AI评估：安全
MD5:	bd324fbbc690f9bc84115e4f151a1087
SHA1:	737b0fe236313a507fd9c49738[illegible]74bf0e199
SHA256:	1b98ec1c738d81db93b26a[illegible]43adc8b88dd97757a[illegible]0ab527d96f2524b0ae2

分析结果严重性分布

高危	中危	信息	安全	关注
9	12	2	1	0

四大组件导出状态统计

Activity组件：3个，其中export的有：0个
Service组件：0个，其中export的有：0个
Receiver组件：1个，其中export的有：0个
Provider组件：3个，其中export的有：0个

应用签名证书信息

APK已签名
v1 签名: True
v2 签名: True
v3 签名: True
v4 签名: False
主题: C=CN, ST=XT应用库, L=小特网, O=星特科技, CN=小特_XT
签名算法: rsassa_pkcs1v15
有效期自: 2025-05-18 11:34:03+00:00
有效期至: 4072-01-07 11:34:03+00:00
发行人: C=CN, ST=XT应用库, L=小特网, O=星特科技, CN=小特_XT
序列号: 0x5fcfdf7e
哈希算法: sha256
证书MD5: 259f172bcb9692517ee05ca7f589d635
证书SHA1: 15212f81e1ae6af539c5e7df8692e76e3e97d833
证书SHA256: 4f97549389e1f66a2c4505a647bf51f57c9fa460d784b3e730a2547474019c58
证书SHA512:
041f2151ff3543fc1188be821e0886e6f6788d98fd1c3a2b79cfe46ae6aee1c31a15cbb64e900b28a76e2e23025cfb36dc8058258046d8fc67714f8efd105394

公钥算法: rsa
密钥长度: 2048
指纹: 5a195cbbedcd080c7f0f32238584125fbd29ab0760a0b764a3f65d4e6972487c
共检测到 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.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.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.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。
android.permission.ACCESS_ALL_DOWNLOADS	未知	未知权限	来自 android 引用的未知权限。
android.permission.ACCESS_BLUETOOTH_SHARE	未知	未知权限	来自 android 引用的未知权限。
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.CHANGE_WIFI_MULTICAST_STATE	危险	允许接收WLAN多播	允许应用程序接收并非直接向您的设备发送的数据包。这样在查找附近提供的服务时很有用。这种操作所耗电量大于非多播模式。
android.permission.CHANGE_WIFI_STATE	危险	改变Wi-Fi状态	允许应用程序改变Wi-Fi状态。
android.permission.READ_INSTALL_SESSIONS	未知	未知权限	来自 android 引用的未知权限。
android.permission.REQUEST_INSTALL_PACKAGES	危险	允许安装应用程序	Android8.0 以上系统允许安装未知来源应用程序权限。
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置方面的数据。恶意应用程序可借此破坏您的系统配置。
android.permission.MANAGE_EXTERNAL_STORAGE	危险	文件列表访问权限	Android11新增权限，读取本地文件，如简历，聊天图片。
android.permission.KILL_BACKGROUND_PROCESSES	普通	结束进程	允许应用程序结束其他应用程序的后台进程。

android.permission.RESTART_PACKAGES	普通	重启进程	允许程序自己重启或重启其他程序
android.permission.PERSISTENT_ACTIVITY	危险	让应用程序始终运行	允许应用程序部分持续运行，这样系统便不能将其用于其他应用程序。
android.permission.POST_NOTIFICATIONS	危险	发送通知的运行时权限	允许应用发布通知，Android 13 引入的新权限。

可浏览 Activity 组件分析

ACTIVITY	INTENT
net.fusionapp.core.WelcomeActivity	Schemes: fusion://,

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: **0** | 警告: **1** | 信息: **1**

标题	严重程度	描述信息
已签名应用	信息	应用已使用代码签名证书进行签名。

Manifest 配置安全分析

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	应用已启用明文网络流量 [android:usesCleartextTraffic=true]	警告	应用允许明文网络流量（如 HTTP、FTP 协议、DownloadManager、MediaPlayer 等）。API 级别 27 及以下默认启用，28 及以上默认禁用。明文流量缺乏机密性、完整性和真实性保护，攻击者可窃听或篡改传输数据。建议关闭明文流量，仅使用加密协议。
2	应用已配置网络安全策略 [android:networkSecurityConfig=@7F120001]	信息	网络安全配置允许应用通过声明式配置文件自定义网络安全策略，无需修改代码。可针对特定域名或应用范围进行灵活配置。
3	应用数据允许备份 [android:allowBackup=true]	警告	该标志允许通过 adb 工具备份应用数据。启用 USB 调试的用户可直接复制应用数据，存在数据泄露风险。

代码安全漏洞检测

高危: **9** | 警告: **9** | 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	SHA-1是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用了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-4	升级会员：解锁高级权限
3	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
4	不安全的Web视图实现。Web视图忽略SSL证书错误并接受任何SSL证书。此应用程序易受MITM攻击	高危	CWE: CWE-295: 证书验证不恰当 OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	升级会员：解锁高级权限
5	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
6	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
7	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
8	已启用远程WebView调试	高危	CWE: CWE-919: 移动应用程序中的弱点 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	升级会员：解锁高级权限
9	应用程序创建临时文件。敏感信息永远不应该被写进临时文件	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

10	该文件是World Readable。任何应用程序都可以读取文件	高危	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
11	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
12	SSL的不安全实现。信任所有证书或接受自签名证书是一个关键的安全漏洞。此应用程序易受MITM攻击	高危	CWE: CWE-295: 证书验证不恰当 OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	升级会员：解锁高级权限
13	MD5是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用了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-4	升级会员：解锁高级权限
14	应用程序使用带PKCS5/PKCS7填充的加密模式CBC。此配置容易受到填充oracle攻击。	高危	CWE: CWE-649: 依赖于混淆或加密安全相关输入而不进行完整性检查 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	升级会员：解锁高级权限
15	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: 使用了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
16	启用了调试配置。生产版本不能是可调试的	高危	CWE: CWE-919: 移动应用程序中的弱点 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	升级会员：解锁高级权限

17	如果一个应用程序使用WebView.loadDataWithBaseURL方法来加载一个网页到WebView，那么这个应用程序可能会遭受跨站脚本攻击	高危	CWE: CWE-79: 在Web页面生成时对输入的转义处理不恰当（'跨站脚本'） OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-6	升级会员：解锁高级权限
18	使用弱加密算法	高危	CWE: CWE-327: 使用了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-4	升级会员：解锁高级权限
19	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
20	可能存在跨域漏洞。在 WebView 中启用从 URL 访问文件可能会泄漏文件系统中的敏感信息	警告	CWE: CWE-200: 信息泄露 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限

应用行为分析

编号	行为	标签	文件
00130	获取当前WIFI信息	WiFi 信息收集	升级会员：解锁高级权限
00033	查询IMEI号	信息收集	升级会员：解锁高级权限
00067	查询IMSI号码	信息收集	升级会员：解锁高级权限
00063	隐式意图（查看网页、拨打电话等）	控制	升级会员：解锁高级权限
00202	打电话	控制	升级会员：解锁高级权限
00203	将电话号码放入意图中	控制	升级会员：解锁高级权限
00051	通过setData隐式意图（查看网页、拨打电话等）	控制	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
00094	连接到 URL 并从中读取数据	命令 网络	升级会员：解锁高级权限
00108	从给定的 URL 读取输入流	网络 命令	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
00121	创建目录	文件 命令	升级会员：解锁高级权限
00125	检查给定的文件路径是否存在	文件	升级会员：解锁高级权限
00013	读取文件并将其放入流中	文件	升级会员：解锁高级权限
00024	Base64解码后写入文件	反射 文件	升级会员：解锁高级权限
00019	从给定的类名中查找方法，通常用于反射	反射	升级会员：解锁高级权限
00029	动态初始化类对象	反射	升级会员：解锁高级权限
00157	使用反射实例化新对象，可能用于 dexClassLoader	反射 dexClassLoader	升级会员：解锁高级权限
00026	方法反射	反射	升级会员：解锁高级权限
00005	获取文件的绝对路径并将其放入 JSON 对象	文件	升级会员：解锁高级权限
00054	从文件安装其他APK	反射	升级会员：解锁高级权限
00076	获取当前WiFi信息并放入JSON中	信息收集 WiFi	升级会员：解锁高级权限
00192	获取短信收件箱中的消息	短信	升级会员：解锁高级权限
00036	从 res/raw 目录获取资源文件	反射	升级会员：解锁高级权限
00004	获取文件名并将其放入 JSON 对象	文件 信息收集	升级会员：解锁高级权限
00014	将文件读入流并将其放入 JSON 对象中	文件	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	2/30	android.permission.REQUEST_INSTALL_PACKAGES android.permission.WRITE_SETTINGS

其它常用权限	6/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.ACCESS_WIFI_STATE android.permission.CHANGE_WIFI_STATE

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。

恶意域名威胁检测

域名	状态	中国境内	位置信息
www.fusionapp.net	安全	是	**IP地址:** 122.51.110.128 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.230416 **经度:** 121.473701 **查看:** 高德地图
h5.m.taobao.com	安全	是	**IP地址:** 58.218.92.191 **国家:** 中国 **地区:** 中国江苏 **城市:** 南京 **纬度:** 32.060255 **经度:** 118.796877 **查看:** 高德地图
mobilegw-1-64.test.alipay.net	安全	否	No Geolocation information available.
mobilegw.aaa.alipay.net	安全	否	No Geolocation information available.
mobilegw.stable.alipay.net	安全	否	No Geolocation information available.

URL 链接安全分析

URL信息	源码文件
• https://mobilegw.alipay.com/mgw.htm • http://mobilegw.aaa.alipay.net/mgw.htm • http://mobilegw-1-64.test.alipay.net/mgw.htm • http://mobilegw.stable.alipay.net/mgw.htm	a/a/c/b/a.java
• https://mobilegw.alipay.com/mgw.htm • http://h5.m.taobao.com/trade/paysuccess.html?bizorderid=$orderid$&	a/a/f/c/b.java
• http://m.alipay.com/?action=h5quit	a/a/f/a/d.java
• https://mcgw.alipay.com/sdklog.do	a/a/f/f/e/b.java
• https://mobilegw.alipay.com/mgw.htm	a/a/a/b/a.java
• http://www.fusionapp.net/	c/a/a/k/v/m.java

• http://h5.m.taobao.com/trade/paysuccess.html?bizorderid=$orderid$&	a/a/f/c/a.java

第三方 SDK 组件分析

SDK名称	开发者	描述信息
cJSON	cJSON	Ultralightweight JSON parser in ANSI C.
AndroLua	mkottman	AndroLua 是基于 LuaJava 开发的安卓平台轻量级脚本编程语言工具，拥有 Lua 简洁优雅的特质，又支持绝大部分安卓 API，可以使你在手机上快速编写小型应用。
Jetpack Lifecycle	Google	生命周期感知型组件可执行操作来响应另一个组件（如 Activity 和 Fragment）的生命周期状态的变化。这些组件有助于您写出更有条理且往往更精简的代码，这样的代码更易于维护。
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。
Jetpack Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。

敏感凭证泄露检测

可能的密钥
aa9852bc5a53272ac8031d49b65e4b0e
e60418c4b638f20d0721e115674ca11f
dab2cead827ef5313f28e22b6fa8479f
3e24e49741b60c215c010dc6048fca7d
44656C69766572792D646174653A
q1w2e3r4t5y6u7i8o9p0a1s2d3f4g5h6j7k8l9z0x1c2v3b4n5m6
b6cbad6cbd5ed0d209a669ad3aa7a617efaae9b3c72a6cc0be42d924936fa78c8001b1fd74b079e5ff9690061dacfa4768e981a526b9ca77156ca36251cf2f906d1054813749963e6e6e18f75ca98b8ed2eaf6ff402c874cca0a263053f22237858206867d210020daa38c48b20cc9dfd82b44a51aeb5db459b22794e2d649

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。