南明离火
移动应用检测平台

ANDROID 静态分析报告

大象视频

大xiang • v2.3.2

分析日期: 2024-04-01 11:22:01

应用概览

文件名称:	大xiang.apk
文件大小:	1.13MB
应用名称:	大xiang
软件包名:	com.bsitoqau.zcepwldf
主活动:	com.win.first.MainActivity
版本号:	2.8.2
最小SDK:	22
目标SDK:	29
加固信息:	未加壳
应用程序安全分数:	53/100 (中风险)
杀软检测:	4 个杀毒软件报毒
MD5:	15b284c26af8fa068f351168eb25f2f1
SHA1:	f0aa9bb9f671db6df15d0617e252c4d5b11e5311
SHA256:	e0a04293f599b60d22ceade08e51c94bb57c0f3d9343612475406d348a2b9fbc

分析结果严重性分布

高危	中危	信息	安全	关注
1	4	0	1	1

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：0个，其中export的有：0个
Provider组件：0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

v4 签名: False
主题: C=C, ST=SR, L=L, O=O, OU=OU, CN=CN
签名算法: rsassa_pkcs1v15
有效期自: 2023-11-09 16:18:41+00:00
有效期至: 2024-11-08 16:18:41+00:00
发行人: C=C, ST=SR, L=L, O=O, OU=OU, CN=CN
序列号: 0x18ee90ee
哈希算法: sha256
证书MD5: 9b958f8e1de9d688c5b9ce38592a3a12
证书SHA1: 9a404d4a13cef160dc0702c079df2f3f67f6690d
证书SHA256: 3e276d41300ff93cd2a70a73ac3e33f49201ff26f2999a2dfd1f735850e01c4f
证书SHA512:
bc94fdae8ca54659fb67f2a188e7efb2c35d5e67056c88099df22748abe9ec9d000eaaf7304fd2352826a7d31982b41ddedf62a9dbc0c2eb5b[illegible]bab3ad97861

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.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.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。

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漏洞的影响。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: **3** | 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 5.1-5.1.1, [minSdk=22]	警告	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。
3	应用程序数据存在被泄露的风险 未设置[android:allowBackup]标志	警告	这个标志 [android:allowBackup]应该设置为false。默认情况下它被设置为true，允许任何人通过adb备份你的应用程序数据。它允许已经启用了USB调试的用户从设备上复制应用程序数据。

代码安全漏洞检测

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

序号	问题	等级	参考标准	文件位置
1	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

敏感权限滥用分析

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	2/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_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
terms.privacypolicy.world	安全	否	**IP地址:** 18.154.144.99 **国家:** United States of America **地区:** Washington **城市:** Seattle **纬度:** 47.627499 **经度:** -122.346199 **查看:** Google 地图
ssl.gstatic.com	安全	否	**IP地址:** 172.217.14.67 **国家:** United States of America **地区:** California **城市:** Mountain View **纬度:** 37.405991 **经度:** -122.078514 **查看:** Google 地图

privacypolicy.bybxmp.com	安全	否	No Geolocation information available.
privacypolicy.yimunongzhuang.net	安全	是	**IP地址:** 58.221.30.135 **国家:** China **地区:** Jiangsu **城市:** Nantong **纬度:** 32.030281 **经度:** 120.874718 **查看:** 高德地图

URL 链接安全分析

URL信息	源码文件
• http://jsperf.com/b64tests • https://github.com/apache/cordova-plugin-whitelist/blob/master/README.md	自研引擎分析结果
• https://privacypolicy.bybxmp.com/data/daxiang • https://privacypolicy.yimunongzhuang.net/data/daxiang • https://terms.privacypolicy.world/data/daxiang	com/win/first/MainActivity.java
• https://www.baidu.com • www.baidu.com	com/win/first/Utils.java
• https://privacypolicy.yimunongzhuang.net/data/daxiang • www.baidu.com • https://terms.privacypolicy.world/data/daxiang • https://www.baidu.com • 127.0.0.255 • https://privacypolicy.bybxmp.com/data/daxiang	自研引擎分析结果

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。