南明离火

移动应用检测平台

ANDROID 静态分析报告

Elixir • v1.1

分析日期: 2024-09-28 11:38:08

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:	Merixti_Injector.apk
文件大小:	5.54MB
应用名称:	Elixir
软件包名:	com.edujoy.kidecats
主活动:	com.androlua.Welcome
版本号:	1.1
最小SDK:	15
目标SDK:	26
加固信息:	未加壳
应用程序安全分数:	28/100 (重大风险)
跟踪器检测:	1/432
杀软检测:	22 个杀毒软件报毒
MD5:	398901064cc6839ebfdbb2ed98f4a21f
SHA1:	7831390345fdf79551b907b0d6eb75ae83bdd3cb
SHA256:	091146b74f82133bfb8d7e5483d3bd1498b04db894fcc0af8160d446937b912

分析结果严重性分布

高危	中危	信息	安全	关注
7	9	1	0	0

四大组件导出状态统计

Activity组件：7个，其中export的有：3个
Service组件：2个，其中export的有：1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

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

v1 签名: True
v2 签名: False
v3 签名: False
v4 签名: False
主题: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
签名算法: rsassa_pkcs1v15
有效期自: 2008-02-29 01:33:46+00:00
有效期至: 2035-07-17 01:33:46+00:00
发行人: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
序列号: 0x936eacbe07f201df
哈希算法: sha1
证书MD5: e89b158e4bcf988ebd09eb83f5378e87
证书SHA1: 61ed377e85d386a8dfee6b864bd85b0bfaa5af81
证书SHA256: a40da80a59d170caa950cf15c18c454d47a39b26989d8b640ecd745ba71bf5dc
证书SHA512:
5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccbe6b34ec4233f5f640703581053abfea3039772720179587704d89b7711292a4569

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.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.UNKNOWN	未知	未知权限	来自 android 引用的未知权限。
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。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.androlua.Main	Schemes: file://, content://, Hosts: *, Mime Types: application/*, audio/*, video/*, text/*, */*,
com.tencent.tauth.AuthActivity	Schemes: tencent222222://,
com.androlua.LuaActivity	Schemes: Elixir://, file://, content://, Hosts: com.edujoy.kidecats, *, Mime Types: text/*,

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**

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

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: **4** | 警告: **5** | 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 4.0.3-4.0.4, [minSdk=15]	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。
3	Activity (com.androlua.Main) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
4	Activity （com.androlua.Main） 容易受到 Android Task Hijacking/StrandHogg 的攻击。	高危	活动不应将启动模式属性设置为“singleTask”。 然后，其他应用程序可以将恶意活动放置在活动栈顶部，从而导致任务劫持/StrandHogg 1.0 漏洞。 这使应用程序成为网络钓鱼攻击的易受攻击目标。 可以通过将启动模式属性设置为“singleInstance”或设置空 taskAffinity (taskAffinity="") 属性来修复此漏洞。 您还可以将应用的目标 SDK 版本 (26) 更新到 28 或更高版本以在平台级别修复此问题。
5	Activity (com.androlua.Main) 未被保护。 存在一个intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。
6	Activity (com.tencent.tauth.AuthActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
7	Activity （com.tencent.tauth.AuthActivity） 容易受到 Android Task Hijacking/StrandHogg 的攻击。	高危	活动不应将启动模式属性设置为“singleTask”。 然后，其他应用程序可以将恶意活动放置在活动栈顶部，从而导致任务劫持/StrandHogg 1.0 漏洞。 这使应用程序成为网络钓鱼攻击的易受攻击目标。 可以通过将启动模式属性设置为“singleInstance”或设置空 taskAffinity (taskAffinity="") 属性来修复此漏洞。 您还可以将应用的目标 SDK 版本 (26) 更新到 28 或更高版本以在平台级别修复此问题。
8	Activity (com.tencent.tauth.AuthActivity) 未被保护。 存在一个intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。
9	Activity (com.androlua.LuaActivity) 未被保护。 存在一个intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。

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

10	Service (com.androlua.LuaAccessibilityService) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.UNKNOWN [android:exported=true]	警告	发现一个 Service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。

代码安全漏洞检测

高危: **2** | 警告: **3** | 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	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
3	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
4	MD5是已知存在哈希冲突的哈希	警告	CWE: CWE-327: 使用已被攻破或存在风险的密码学算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
5	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
6	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

敏感权限滥用分析

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

类型	匹配	权限
恶意软件常用权限	0/30	
其它常用权限	4/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.WRITE_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。

恶意域名威胁检测

域名	状态	中国境内	位置信息
www.objectweb.org	安全	否	No Geolocation information available.

URL 链接安全分析

URL信息	源码文件
• http://crl.microsoft.com/pki/crl/products/MicrosoftTimeStampPCA.crl0X • http://www.microsoft.com/pki/certs/MicrosoftTimeStampPCA.crt0 • http://www.microsoft.com/pki/certs/MicRooCerAut2011_2011_03_22.crt0 • http://crl.microsoft.com/pki/crl/products/microsoftrootcert.crl0T • http://crl.microsoft.com/pki/crl/products/MicRooCerAut2011_2011_03_22.crl0 • http://www.microsoft.com/typography/fonts/ • http://www.microsoft.com/pkiops/certs/MicCodSigPCA2011_2011-07-08.crt0 • http://www.microsoft.com/pkiops/crl/MicCodSigPCA2011_2011-07-08.crl0a • http://www.microsoft.com/pki/certs/MicrosoftRootCert.crt0 • http://www.microsoft.com/Typography • http://www.microsoft.com/pkiops/docs/primarycps.htm0	自研引擎-A
• www.objectweb.org	bsh/ClassGeneratorUtil.java

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

• 3.9.5.4 • http://hmma.baidu.com/app.gif • http://qzs.qq.com/open/mobile/login/qzsjump.html? • http://qzs.qq.com/open/mobile/invite/sdk_invite.html? • http://qzs.qq.com/open/mobile/request/sdk_request.html? • 10.0.0.200 • https://openmobile.qq.com/ • https://openmobile.qq.com/oauth2.0/m_authorize? • http://appsupport.qq.com/cgi-bin/qzapps/mapp_addapp.cgi • www.objectweb.org • http://fusion.qq.com/cgi-bin/qzapps/unified_jump?appid=%1$s&from=%2$s&isopenappid=1 • http://cgi.connect.qq.com/qqconnectopen/openapi/policy_conf • http://qzs.qq.com/open/mobile/sendstory/sdk_sendstory_v1.3.html? • https://graph.qq.com/oauth2.0/me • https://openmobile.qq.com/user/user_login_statis • http://qzs.qq.com • http://openmobile.qq.com/oauth2.0/m_jump_by_version? • https://wspeed.qq.com/w.cgi • javascript:window.jsbridge&&jsbridge.callback • 10.0.0.172 • https://hmma.baidu.com/app.gif • https://hmma.baidu.com/auto.gif • https://openmobile.qq.com/v3/user/get_info • https://huatuocode.huatuo.qq.com • https://appsupport.qq.com/cgi-bin/appstage/mstats_batch_report	自研引擎-S

第三方 SDK 组件分析

SDK名称	开发者	描述信息
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，既具有 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。
腾讯开放平台	Tencent	腾讯核心内部服务，二十年技术沉淀，助你成就更高梦想。
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。

邮箱地址敏感信息提取

EMAIL	源码文件
pat@pat.net	bsh/Interpreter.java
pat@pat.net	自研引擎-S

第三方追踪器检测

名称	类别	网址
Baidu Mobile Stat	Analytics	https://reports.exodus-privacy.eu.org/trackers/101

敏感凭证泄露检测

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

可能的密钥
44656C69766572792D646174653A

Google Play 应用市场信息

标题: Kid-E-Cats. Educational Games

评分: 3.9486585 **安装:** 10,000,000+ **价格:** 0 **Android版本支持:** **分类:** 教育 **Play Store URL:** com.edujoy.kidecats

开发者信息: AppQuiz, 5704336914526446295, c/Ugasko bidea, n3 bis, 2dcha izq 48014 Bilbao, http://edujoy.es, edujoy@edujoy.es,

发布日期: 2019年12月3日 **隐私政策:** Privacy link

关于此应用:

在Kid e Cats的教育游戏中玩得开心并学习！ Edujoy 展示了超过25个有趣的游戏集合，针对2至8岁的儿童开发不同的技能并激发创造力。 所有游戏均由著名国际电视连续剧Kid-E-Cats中的逗猫主演。孩子们可以在糖果、饼干和布丁等角色的陪伴下发展学习技能。喵-哇！ 游戏类型 - 拼图：通过做有趣的拼图来了解世界各国。 - 数学和数字：执行简单的运算并学习数字。 - 视觉感知：通过教育游戏锻炼视觉技能。 - 绘画和涂色：通过创作自己的艺术作品，制作多彩的马赛克并唤醒您的创造力。 - 记忆游戏：找到合适的匹配和更多游戏来刺激视觉记忆。 - 演绎游戏：完整的逻辑元素系列。 - 迷宫：找到正确的迷宫出口，激发注意力。 - 协调：通过协调游戏锻炼精细运动技能 - 单词和字母：学习新单词并享受单词搜索的乐趣。 - 钢琴：用钢琴创作旋律，展示您的音乐技巧。 Kid-e-Cats故事专为学龄前儿童设计。小猫的快乐冒险强调儿童的社交和情感发展，特别注重友谊、家庭和行动前的思考。 应用程序功能 - 20个教育性和互动性游戏 - 惊人的设计和角色，动画和有趣的声音 - 简单直观的儿童界面 - 激发想象力和创造力 - 刺激精细运动技能 - 游戏完全免费 关于益度 非常感谢您玩Edujoy游戏。我们喜欢为所有年龄段的儿童创造有趣的教育游戏。如果您对Kid-E-Cats教育游戏有任何疑问或建议，可以通过开发者的联系方式或我们的社交媒体资料与我们联系： 推特：twitter.com/edujoygames 脸书：facebook.com/edujoysl

---

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