南明离火
移动应用检测平台

ANDROID 静态分析报告

ClevrSyno Pro • v15.1

分析日期: 2025-05-15 14:35:23

应用概览

文件名称:	ClevrSyno.apk
文件大小:	22.83MB
应用名称:	ClevrSyno Pro
软件包名:	com.customscopecommunity.crosshairpro
主活动:	com.e4a.runtime.android.StartActivity
版本号:	15.1
最小SDK:	17
目标SDK:	30
加固信息:	360加固
开发框架:	E4A(易安卓)
应用程序安全分数:	52/100 (中风险)
杀软检测:	7 个杀毒软件报毒
MD5:	990667aca69b50b26e6f09e2b9aa5067
SHA1:	5277d8e0f592299d0d1d4084[illegible]3fb4252c1
SHA256:	5cab66ff7a572f3a2bb609[illegible]393ce4dde15db[illegible]aa9532f05599300dfb6

分析结果严重性分布

高危	中危	信息	安全	关注
1	5	1	1	0

四大组件导出状态统计

Activity组件：2个，其中export的有：1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

APK已签名
v1 签名: True
v2 签名: True
v3 签名: False
v4 签名: False
主题: C=CN, ST=JiangXi, L=NanChang, O=java, OU=java, CN=Riyu
签名算法: rsassa_pkcs1v15
有效期自: 2023-08-24 13:53:18+00:00
有效期至: 4758-10-25 13:53:18+00:00
发行人: C=CN, ST=JiangXi, L=NanChang, O=java, OU=java, CN=Riyu
序列号: 0x4f5b2209
哈希算法: sha1
证书MD5: 481042eb8a90a0f5b04cc5969371e084
证书SHA1: 06ce20b9d4ea92814910def786034e14938db32f
证书SHA256: dbafbd065d8c478e3f2c799545a57618c13e8681a40dc0a79756d54c7590dc23
证书SHA512:
9a23eba3cb979dd7b83e8c50e387292732554b62250f958258f9a0527fde2dfa58dcdd8f9429ffe78c1998f4272969fcacd304f2ea7841ec48a351f625e50c2a

公钥算法: rsa
密钥长度: 2048
指纹: fdd5b6dd399619ac38f0ad04c433c4eca306e6eeefe6d28bce26f26daa3b02b6
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
com.android.launcher.permission.READ_SETTINGS	危险	读取桌面快捷方式	这种权限的作用是允许应用读取桌面快捷方式的设置。
android.permission.CHANGE_CONFIGURATION	危险	修改UI设置	允许应用程序允许应用程序更改当前配置，例如语言区域或整体的字体大小。
android.permission.FOREGROUND_SERVICE	普通	创建前台Service	Android 9.0以上允许常规应用程序使用 Service.startForeground，用于podcast播放（推送悬浮播放，锁屏播放）
android.permission.VIBRATE	普通	控制振动器	允许应用程序控制振动器，用于消息通知振动功能。
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。
android.permission.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序装载和卸载可移动存储器的文件系统。
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.SYSTEM_OVERLAY_WINDOW	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.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.GET_TASKS	危险	检索当前运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。恶意应用程序可借此发现有关其他应用程序的保密信息。
android.permission.WAKE_LOCK	危险	防止手机休眠	允许应用程序防止手机休眠，在手机屏幕关闭后后台进程仍然运行。
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.MODIFY_AUDIO_SETTINGS	危险	允许应用修改全局音频设置	允许应用程序修改全局音频设置，如音量。多用于消息语音功能。
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。
com.android.launcher.permission.INSTALL_SHORTCUT	签名	创建快捷方式	这个权限是允许应用程序创建桌面快捷方式。
android.permission.LAUNCHER	未知	未知权限	来自 android 引用的未知权限。
android.permission.QUERY_ALL_PACKAGES	普通	获取已安装应用程序列表	Android 11引入与包可见性相关的权限，允许查询设备上的任何普通应用程序，而不考虑清单声明
android.permission.REQUEST_DELETE_PACKAGES	普通	请求删除应用	允许应用程序请求删除包。
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。

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: **1** | 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	Activity (com.e4a.runtime.android.mainActivity) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
3	Activity (com.e4a.runtime.android.mainActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。

代码安全漏洞检测

高危: **0** | 警告: **2** | 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	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

应用行为分析

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
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
00191	获取短信收件箱中的消息	短信	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
00036	从 res/raw 目录获取资源文件	反射	升级会员：解锁高级权限
00012	读取数据并放入缓冲流	文件	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
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

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	7/30	android.permission.VIBRATE android.permission.SYSTEM_ALERT_WINDOW android.permission.REQUEST_INSTALL_PACKAGES android.permission.GET_TASKS android.permission.WAKE_LOCK android.permission.MODIFY_AUDIO_SETTINGS android.permission.WRITE_SETTINGS

其它常用权限	7/46	android.permission.FOREGROUND_SERVICE android.permission.WRITE_EXTERNAL_STORAGE android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.READ_EXTERNAL_STORAGE com.android.launcher.permission.INSTALL_SHORTCUT

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
360 加固	360	360 加固保是基于 360 核心加密技术，给安卓应用进行深度加密、加壳保护的安全技术产品，可保护应用远离恶意破解、反编译、二次打包，内存抓取等威胁。
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。

敏感凭证泄露检测

可能的密钥
1CF03B1A165AB57E082714DEBA7A256EB22B19B4D9485682C[illegible]72C6F4A2C6D58030A[illegible]1CDE1EC6F356A3666C14A16AC225352E4A088A4FEBE1BF0B2AD68
416945C72D77E1CB15C7CB422DD646FECF6DC3F4AD86413[illegible]71BACFCCDEFB456[illegible]140A0[illegible]E0EF757E4332C13123C8E92E71BB23AB1279EF92741D0A515044E
0aab637105432c253ff1b416310cd215
4DF54882AA9BEE88753EB7400B117[illegible]A40EA63FEBBE0D16823[illegible]12A3F923CAE484
851CB73A9367B840E9E18718[illegible]7847EC65F42EA2420DD[illegible]951CEE98062D1500611F06752F714EA5A523D13C84872059E622F86FEA93C40ECAE438C6508A687C
56806278ACFFF3E8B[illegible]F[illegible]D54C315EBE12E61[illegible]5490471BA6679CC0A4CEF75BD6
9472BF8183[illegible]A[illegible]137B2099DD8EE7D[illegible]1881CD69E639BED2F98617C69E112E9348B6228A03A69EB1736748033881B
32A6E0[illegible]13DA9AE3B5DDAC7BA[illegible]1E3EE477A39A03899834507FAC2B668C2347360A10575717A8F187A54F98DCD03DA1D739C2E949C8B89CF5723
0E5F77628A263A5C18D[illegible]BF98ACDAC4CBAB12B72941E1E7FEE83A3149ABBEA9B823F0C2609C7
A86AE0E30854D[illegible]66B665D95DDFF7BA6273D2DE23671A745786C4BAE6C5E381EA556086D2CD3F2CB620B18EC455C94D95566458EBBFAD541489238095F8A4[illegible]
3AF74DF[illegible]E[illegible]5D644119811E61A95E54652252C640FEB9612008F918AD462F64F47D0F83F47C47025EBE49BA1D61F214DD0E2FC1FA65F0AE116EC7143D2
D52E2A3A4CD6FF87A09436797AAF1B63CE91922BB0A92A590EFAC69D4749F0622C

70381826F76F8C6230B309135E3888F987C4284B2210F4AC13AB72765DE666F99C22601B153940E1CC411251033D34012CAE2EB9F56CFDCB9AC9
FC3516C66379F455DF9136E1265DCD6ECAF6BD7CE47DB8E376E956D92F94461C46ECB9

Google Play 应用市场信息

标题: Crosshair Pro: Custom Scope

评分: 4.2153406 **安装:** 5,000,000+ **价格:** 0 **Android版本支持:** **分类:** 工具 **Play Store URL:** com.customscopecommunity.crosshairpro

开发者信息: Pipi Chick Studio, 5434220716348776313, Kempinski 16, Rishon Lezion, https://pipichickstudio.com/crosshairpro, support.crosshairpro@pipichickstudio.com,

发布日期: 2019年9月7日 **隐私政策:** Privacy link

关于此应用:

Crosshair Pro：自定义您的瞄准镜，实现更清晰的瞄准！Crosshair Pro：自定义瞄准镜非常适合任何级别的战略家，也可以帮助您在任何 FPS 中获得优势，Crosshair Pro：自定义瞄准镜将精确瞄准提升到一个新的水平。您保持正轨、瞄准目标、提高射击技巧所需的所有工具都在这里，只需单击一下即可。Crosshair Pro 自定义瞄准镜可帮助所有在预装瞄准镜方面遇到困难或希望在竞技舞台上更快地提高游戏水平的玩家。 Crosshair Pro：自定义瞄准镜在可视性、准确性和整体性能增强方面取得了惊人的改进，消除了您的所有后顾之忧。是时候放弃默认设置并开始展示您的专业级目标了。 Crosshair Pro：自定义瞄准镜功能： 在默认不可用的游戏中设置 FPS 十字线； 完全可调节的设计并设置尺寸、形状甚至颜色和透明度； 在自定义十字线 v2 中，可以访问多种预制选项； 对于游戏，使用 Crosshair X 在所有物体上覆盖精确的瞄准镜； 将十字线定位在屏幕上的任意位置，并在游戏过程中实时调整； 各大FPS游戏完美兼容； 访问经典和专业套装来匹配和打造您的拍摄风格； 要有效地定制您的目标，请使用自定义十字线 v2 编辑器； 这可以通过增强焦点和精确度来帮助解决视力问题的用户； 借助 FPS 十字线，在任何射击游戏中实现狙击手级精准度。 提高每个 FPS 的战斗准确性！Crosshair Pro：自定义瞄准镜对于寻求完全控制目标的游戏玩家来说是最佳选择。与有限的游戏内设置不同，该工具提供了修改视线的完全自由。 Crosshair X For Games 提供立即激活高精度叠加的选项，从而更快、更准确地瞄准敌人。无论是配备基础枪械还是狙击手，该工具都提供了无与伦比的精准度优势。 自定义十字线 v2 允许微调透明度和颜色等元素，提供更好的可见性。这对于视觉受限的用户或游戏玩家的 Cross Hairs For FPS 体验非常有效。 通用自定义范围： Crosshair Pro：自定义范围不限于标题；它与许多 FPS 游戏交互。在方便的半径内添加十字准线以提高 FPS，甚至无瞄准镜枪支也会变得强大。使用 Crosshair X For Games 在所有 FPS 游戏中占据主导地位，从而获得优势。 职业玩家和新手最好的朋友： 从初学者到成熟的 FPS 爱好者，每个人都可以得到 Crosshair Pro：自定义瞄准镜的帮助。使用 Crosshairs For FPS 提高您的技能，使用 Custom Crosshair v2 个性化您的叠加层，并使用 Crosshair X For Games 释放终极统治潜力。每个人都会犯错，别再投丢球了。 立即开始您的精准射击之旅！获取 Crosshair Pro：自定义瞄准镜，同时提高您的射击精度。无论您喜欢用 Crosshair X For Games 的 CGV 方式表达，还是依靠 Custom Crosshair v2 来设定您的目标。使用 Cross Hairs For FPS 控制行动，在战场上获得无与伦比的火力。唯一的问题是，你希望下一个目标在哪里？

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。