南明离火
移动应用检测平台

ANDROID 静态分析报告

Cricket Line Guru v20.2

分析日期: 2025-04-05 07:53:01

应用概览

文件名称:	Cricket Line Guru v20.2.apk
文件大小:	18.07MB
应用名称:	Cricket Line Guru
软件包名:	com.app.cricketapp
主活动:	com.app.cricketapp.features.main.MainActivity
版本号:	20.2
最小SDK:	23
目标SDK:	34
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	47/100 (中风险)
跟踪器检测:	10/432
杀软检测:	经检测，该文件安全
MD5:	0afc9f3596b95c7e814b224528ae0a2c
SHA1:	52a325f6a861bdc4e2ae427ec3e1660179f9831f
SHA256:	33a956c2115a6f7[illegible]dc5[illegible]611f61f3448065840d4cad2b28b71c4ce88ad2e9

分析结果严重性分布

高危	中危	信息	安全	关注
7	37	4	3	1

四大组件导出状态统计

Activity组件：42个，其中export的有： 22个
Service组件：19个，其中export的有： 3个
Receiver组件：14个，其中export的有： 3个
Provider组件：7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: True
v3 签名: True
v4 签名: False
主题: CN=Hello
签名算法: rsassa_pkcs1v15
有效期自: 2017-05-06 05:30:49+00:00
有效期至: 2042-04-30 05:30:49+00:00
发行人: CN=Hello
序列号: 0x64094111
哈希算法: sha256
证书MD5: d8342dbef29bc3fda0edb6bb1ca35a4a
证书SHA1: 2fe17a6071b438417eefe5435f1be15a02573a00
证书SHA256: 3be9d9da54a844d069597c2efe2a7a0cb663b4db0262acbd1cff22dc5d46702c
证书SHA512:
20954000d6d111c4fd0f956d865cc009a946969d33c850fcb4b46407093938d2ed5cb56c97448ef5e4168a7a7519cf93c1917005d7a31c7475e64e2741ddf077

公钥算法: rsa
密钥长度: 2048
指纹: d92c3b9e323fbbd300832d3f2344bc24b76907302812670c7a9bc646e26f2a10
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.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.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.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。
com.google.android.c2dm.permission.RECEIVE	普通	接收推送通知	允许应用程序接收来自云的推送通知。
com.google.android.gms.permission.AD_ID	普通	应用程序显示广告	此应用程序使用 Google 广告 ID，并且可能会投放广告。
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.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.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。
android.permission.READ_PHONE_STATE	危险	读取手机状态和标识	允许应用程序访问设备的手机功能。有此权限的应用程序可确定此手机的号码和序列号，是否正在通话，以及对方的号码等。
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	普通	允许应用程序访问广告服务归因	这使应用能够检索与广告归因相关的信息，这些信息可用于有针对性的广告目的。应用程序可以收集有关用户如何与广告互动的数据，例如点击或展示，以衡量广告活动的有效性。
android.permission.ACCESS_ADSERVICES_AD_ID	普通	允许应用访问设备的广告 ID。	此 ID 是 Google 广告服务提供的唯一、用户可重置的标识符，允许应用出于广告目的跟踪用户行为，同时维护用户隐私。
android.permission.ACCESS_ADSERVICES_TOPICS	普通	允许应用程序访问广告服务主题	这使应用程序能够检索与广告主题或兴趣相关的信息，这些信息可用于有针对性的广告目的。

com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	普通	Google 定义的权限	由 Google 定义的自定义权限。
com.app.cricketapp.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	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。
com.android.vending.CHECK_LICENSE	未知	未知权限	来自 android 引用的未知权限。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.app.cricketapp.features.home.HomeActivity	Schemes: https://, Hosts: www.cricketlineguru.com, Path Prefixes: /cricket-news,
com.google.firebase.auth.internal.GenericIdpActivity	Schemes: genericidp://, Hosts: firebase.auth, Paths: /,
com.google.firebase.auth.internal.RecaptchaActivity	Schemes: recaptcha://, Hosts: firebase.auth, Paths: /,
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.com.app.cricketapp,

网络通信安全风险分析

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

序号	范围	严重级别	描述
1	127.0.0.1 34.171.208.160 13.235.13.153 qa.commentaryapi.com dev.cricketlineguru.com	高危	域配置不安全地配置为允许明文流量到达范围内的这些域。

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	应用程序使用代码签名证书进行签名

Manifest 配置安全分析

高危: **0** | 警告: **29** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息

本报告由南明离火移动安全分析平台生成

1	应用程序具有网络安全配置 [android:networkSecurityConfig=@xml/network_security_config]	信息	网络安全配置功能让应用程序可以在一个安全的，声明式的配置文件中自定义他们的网络安全设置，而不需要修改应用程序代码。这些设置可以针对特定的域名和特定的应用程序进行配置。
2	Activity (com.app.cricketapp.features.home.HomeActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
3	Activity (com.app.cricketapp.features.redeem.RedeemActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
4	Activity (com.app.cricketapp.features.venue.detail.VenueDetailActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
5	Activity (com.app.cricketapp.features.stats.StatsActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
6	Activity (com.app.cricketapp.features.login.LoginActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
7	Activity (com.app.cricketapp.features.premium.subscription.SubscriptionPlansActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
8	Activity (com.app.cricketapp.features.team.detail.TeamsDetailActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
9	Activity (com.app.cricketapp.features.webView.WebViewActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
10	Activity (com.app.cricketapp.features.ranking.RankingActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
11	Activity (com.app.cricketapp.features.player.playerList.PlayerListActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
12	Activity (com.app.cricketapp.features.team.list.TeamsActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。

13	Activity (com.app.cricketapp.features.series.list.SeriesActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
14	Activity (com.app.cricketapp.features.fixtures.detail.FixtureDetailActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
15	Activity (com.app.cricketapp.features.series.detail.SeriesDetailActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
16	Activity (com.app.cricketapp.features.news.list.NewsListActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
17	Activity (com.app.cricketapp.features.news.detail.NewsDetailActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
18	Activity (com.app.cricketapp.features.player.profile.PlayerProfileActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
19	Activity (com.app.cricketapp.features.squad.SquadActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
20	Activity (com.app.cricketapp.features.matchLine.MatchLineActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
21	Service (com.app.cricketapp.firebase.services.NotificationService) 未被保护。 [android:exported=true]	警告	发现 Service与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
22	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) 受权限保护，但是应该检查权限的保护级别。 Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	警告	发现一个 Broadcast Receiver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。
23	Activity (com.google.firebase.auth.internal.GenericIdpActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。

24	Activity (com.google.firebase.auth.internal.RecaptchaActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
25	Activity (com.facebook.CustomTabActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
26	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) 受权限保护, 但是应该检查权限的保护级别。 Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [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。
27	Service (androidx.work.impl.background.systemjob.SystemJobService) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.BIND_JOB_SERVICE [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。
28	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.DUMP [android:exported=true]	警告	发现一个 Broadcast Receiver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。
29	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.DUMP [android:exported=true]	警告	发现一个 Broadcast Receiver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: **5** | 警告: **3** | 信息: **3** | 安全: **2** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	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

2	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
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	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
5	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
6	不安全的Web视图实现。可能存在WebView任意代码执行漏洞	警告	CWE: CWE-749: 暴露危险方法或函数 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	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	此应用程序使用SSL Pinning 来检测或防止安全通信通道中的MITM攻击	安全	OWASP MASVS: MSTG-NETWORK-4	升级会员：解锁高级权限
9	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

10	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
11	此应用程序可能具有Root检测功能	安全	OWASP MASVS: MSTG-RESILIENCE-1	升级会员：解锁高级权限
12	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
13	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
14	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
15	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
16	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: 依靠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
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	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

应用行为分析

编号	行为	标签	文件
00078	获取网络运营商名称	信息收集 电话服务	升级会员：解锁高级权限
00171	将网络运算符与字符串进行比较	网络	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
00036	从 res/raw 目录获取资源文件	反射	升级会员：解锁高级权限
00092	发送广播	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
00096	连接到 URL 并设置请求方法	命令 网络	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
00163	创建新的 Socket 并连接到它	socket	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
00091	从广播中检索数据	信息收集	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
00112	获取日历事件的日期	信息收集 日历	升级会员：解锁高级权限
00046	方法反射	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
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
00028	从assets目录中读取文件	文件	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
00026	方法反射	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
00162	创建 InetSocketAddress 对象并连接到它	socket	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
00191	获取短信收件箱中的消息	短信	升级会员：解锁高级权限
00001	初始化位图对象并将数据（例如JPEG）压缩为位图对象	相机	升级会员：解锁高级权限
00077	读取敏感数据（短信、通话记录等）	信息收集 短信 通话记录 日历	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
00166	获取短信正文并从中检索字符串（可能是 PIN / mTAN）	短信 PIN码	升级会员：解锁高级权限
00114	创建到代理地址的安全套接字连接	网络 命令	升级会员：解锁高级权限
00034	查询当前数据网络类型	信息收集 网络	升级会员：解锁高级权限
00132	查询ISO国家代码	电话服务 信息收集	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
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

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	4/30	android.permission.WAKE_LOCK android.permission.SYSTEM_ALERT_WINDOW android.permission.VIBRATE android.permission.READ_PHONE_STATE
其它常用权限	7/46	android.permission.ACCESS_NETWORK_STATE android.permission.INTERNET com.google.android.c2dm.permission.RECEIVE com.google.android.gms.permission.AD_ID android.permission.FOREGROUND_SERVICE com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE android.permission.ACCESS_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

clgphase2.cricketlineguru.in	安全	否	No Geolocation information available.
easypay.paytm.com	安全	否	No Geolocation information available.
ads.inmobi.com	安全	否	**IP地址:** 185.199.108.153 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
www.cricketlineguru.com	安全	否	**IP地址:** 34.120.206.254 **国家:** 印度 **地区:** 马哈拉施特拉邦 **城市:** 孟买 **纬度:** 19.075975 **经度:** 72.877380 **查看:** Google 地图
spadsync.com	安全	否	**IP地址:** 34.49.219.143 **国家:** 美国 **地区:** 密苏里州 **城市:** 堪萨斯城 **纬度:** 39.099731 **经度:** -94.578568 **查看:** Google 地图
comm-panel.s3.ap-south-1.amazonaws.com	安全	否	**IP地址:** 199.101.153.122 **国家:** 印度 **地区:** 马哈拉施特拉邦 **城市:** 孟买 **纬度:** 19.075975 **经度:** 72.877380 **查看:** Google 地图
www.fyber.com	安全	否	**IP地址:** 151.101.3.52 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
secure4.arcot.com	安全	否	**IP地址:** 34.49.219.143 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 圣何塞 **纬度:** 37.385639 **经度:** -121.885277 **查看:** Google 地图
sachin.webscript.io	安全	否	No Geolocation information available.
criclive-7[illegible]dee.firebaseio.com	安全	否	**IP地址:** 34.120.206.254 **国家:** 美国 **地区:** 密苏里州 **城市:** 堪萨斯城 **纬度:** 39.099731 **经度:** -94.578568 **查看:** Google 地图

config.inmobi.com	安全	否	**IP地址:** 34.49.219.143 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
i.l.inmobicdn.net	安全	否	**IP地址:** 34.49.219.143 **国家:** 美国 **地区:** 密苏里州 **城市:** 堪萨斯城 **纬度:** 39.099731 **经度:** -94.578568 **查看:** Google 地图
log-activity.templates.inmobi.com	安全	否	**IP地址:** 34.49.219.143 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
dashif.org	安全	否	**IP地址:** 34.49.219.143 **国家:** 美国 **地区:** 宾夕法尼亚 **城市:** 加利福尼亚 **纬度:** 40.065647 **经度:** -79.891724 **查看:** Google 地图
cricketguru.atmegame.com	安全	否	**IP地址:** 104.22.2.151 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
unif-id.ssp.inmobi.com	安全	否	**IP地址:** 199.101.153.122 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
twitter.com	安全	否	**IP地址:** 172.66.0.227 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
init-mp.fyber.com	安全	否	**IP地址:** 34.49.219.143 **国家:** 美国 **地区:** 密苏里州 **城市:** 堪萨斯城 **纬度:** 39.099731 **经度:** -94.578568 **查看:** Google 地图

securegw.paytm.in	安全	否	**IP地址:** 23.48.185.212 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 洛杉矶 **纬度:** 34.052570 **经度:** -118.243904 **查看:** Google 地图
securegw-preprod.paytm.in	安全	否	**IP地址:** 23.61.209.156 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 埃尔塞贡多 **纬度:** 33.919201 **经度:** -118.416530 **查看:** Google 地图
telemetry.sdk.inmobi.com	安全	否	**IP地址:** 35.212.28.21 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
itunes.apple.com	安全	是	**IP地址:** 14.29.219.143 **国家:** 中国 **地区:** 江苏 **城市:** 扬州 **纬度:** 32.397221 **经度:** 119.435600 **查看:** 高德地图
crash-metrics.sdk.inmobi.com	安全	否	**IP地址:** 35.212.101.248 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
cricketguru.atmequiz.com	安全	否	**IP地址:** 104.22.36.90 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
cdn2.inner-active.mobi	安全	否	**IP地址:** 151.101.195.52 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
www.inmobi.com	安全	否	**IP地址:** 20.81.69.107 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 华盛顿 **纬度:** 38.713848 **经度:** -78.159439 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• https://cricketguru.atmequiz.com/start • https://cricketguru.atmegame.com/online-cricket-games • https://clgphase2.cricketlineguru.in/terms-and-conditions • https://comm-panel.s3.ap-south-1.amazonaws.com/config/app-3.json • https://clgphase2.cricketlineguru.in/privacy-policy	m4/a.java
• http://www.fyber.com	com/fyber/inneractive/sdk/click/j.java
• https://play.google.com/store/apps/details?id=	com/fyber/inneractive/sdk/click/e.java
• https://%sconfig_android.json	com/fyber/inneractive/sdk/cache/d.java
• https://%sfeatures_config.json	com/fyber/inneractive/sdk/config/global/m.java
• https://github.com/firebase/firebase-android-sdk • https://firebase.google.com/docs/database/ios/structure-data#best_practices_for_data_structure • https://firebase.google.com/docs/database/android/retrieve-data#filtering_data	bn/k.java
• https://cdn2.inner-active.mobi/client/fyber-i-icon/index.html	com/fyber/inneractive/sdk/activities/FyberReportAdActivity.java
• http://www.cricketlineguru.com/cricket-news/ • http://www.cricketlineguru.com/	com/app/cricketapp/models/DeepLinkURLS.java
• www.cricketlineguru.com	v7/d.java
• data:a.data}};function	com/inmobi/media/m9.java
• https://init-mp.fyber.com/init	com/fyber/inneractive/sdk/network/k0.java
• https://play.google.com/store/apps/details?id=com.app.cricketapp	h5/c.java
• https://play.google.com/store/apps/details?id=com.app.cricketapp	h5/b.java
• https://itunes.apple.com/in/app/cricket-line-guru/id1247859253?mt=8	ne/n.java
• https://config.inmobi.com/config-server/v1/config/secure.cfg	com/inmobi/commons/core/configs/RootConfig$ComponentConfig.java
• https://crash-metrics.sdk.inmobi.com/trace	com/inmobi/commons/core/configs/CrashConfig.java
• https://www.inmobi.com/products/sdk/#downloads	com/inmobi/commons/core/configs/RootConfig$LatestSdkInfo.java
• https://config.inmobi.com/config-server/v1/config/secure.cfg	com/inmobi/commons/core/configs/RootConfig.java
• javascript:document.body.style.setproperty	com/app/cricketapp/features/webView/WebViewActivity$b.java
• http://www.google.com	com/inmobi/media/f3.java

• https://i.l.inmobicdn.net/sdk/sdk/1058/android/mraid.js • https://ads.inmobi.com/sdk • https://i.l.inmobicdn.net/sdk/sdk/omid/omsdk-v1.3.17.js	com/inmobi/commons/core/configs/AdConfig.java
• https://log-activity.templates.inmobi.com/api/v1/ingest	com/inmobi/commons/core/configs/TelemetryConfig$LoggingConfig.java
• https://telemetry.sdk.inmobi.com/metrics	com/inmobi/commons/core/configs/TelemetryConfig.java
• https://spadsync.com/sync	com/inmobi/commons/core/configs/SignalsConfig$NovatiqConfig.java
• https://cdn2.inner-active.mobi/app-detail-page-v0/	com/fyber/inneractive/sdk/flow/p.java
• https://unif-id.ssp.inmobi.com/fetch	com/inmobi/commons/core/configs/SignalsConfig.java
• https://securegw.paytm.in/merchant-settlement-service/paytmassist/enable	easypay/appinvoke/manager/PaytmAssist$2.java
• https://securegw.paytm.in/payassist/api/submit/event/logs	easypay/appinvoke/utils/AnalyticsService.java
• https://securegw.paytm.in/payassist/api/geturlbyappversion	easypay/appinvoke/manager/PaytmAssist$1.java
• https://console.firebase.google.com/	dp/m.java
• https://twitter.com	u6/c.java
• https://play.google.com/store/apps/details?id=com.app.cricketapp	p8/b.java
• javascript:fybermraidvideotracker.initomid • javascript:fybermraidvideotracker.impression • javascript:fybermraidvideotracker.aduserinteraction	com/fyber/inneractive/sdk/measurement/tracker/b.java
• http://dashif.org/guidelines/trickmode • http://dashif.org/guidelines/last-segment-number	yi/d.java
• https://firebase.google.com/support/privacy/init-options	ko/e.java
• https://config.inmobi.com/config-server/v1/config/secure.cfg	com/inmobi/media/r2$a.java
• https://secure4.arcot.com/acspage/cap?rid=10147&vaa=b	mq/a.java
• https://cdn2.inner-active.mobi/ia-jstag/production/centering_v1.js • https://cdn2.inner-active.mobi/client/ia-js-tags/dt-mraid-video-controller.js • https://cdn2.inner-active.mobi/ia-jstag/production/centering_v1.css	com/fyber/inneractive/sdk/web/e.java
• https://cdn2.inner-active.mobi/client/ia-js-tags/omsdk/omid-session-client-%s.js • https://cdn2.inner-active.mobi/client/ia-js-tags/omsdk/%s.js • https://cdn2.inner-active.mobi/client/ia-js-tags/omsdk/dt-omsdk-mraid-video-tracker.js	com/fyber/inneractive/sdk/measurement/b.java
• https://cdn2.inner-active.mobi/ia-jstag/production/centering_v1.js • https://cdn2.inner-active.mobi/client/ia-js-tags/dt-mraid-video-controller.js • https://cdn2.inner-active.mobi/ia-jstag/production/centering_v1.css	com/fyber/inneractive/sdk/cache/i.java
• https://securegw.paytm.in/theia/api/v1/showpaymentpage	cq/n.java

本报告由南明离火移动安全分析平台生成

• https://securegw.paytm.in/payassist/api/geturlbyappversion • https://securegw.paytm.in/payassist/api/submit/event/logs • https://securegw-preprod.paytm.in/payassist/api/getuniqueassist • https://securegw.paytm.in/merchant-settlement-service/paytmassist/enable	easypay/appinvoke/manager/Constants.java
• https://%s/%s/%s	no/c.java
• https://easypay.paytm.com/paytmanalytics/logerror • http://sachin.webscript.io/sachin • https://www.instagram.com/cricketlineguru.official • https://easypay.paytm.com/paytmanalytics/logevent • https://www.facebook.com/cricketlineguru.in • http://play.google.com/store/apps/details?id=%1s • https://criclive-72dee.firebaseio.com • https://play.google.com/store/apps/details?id=com.app.cricketapp	自研引擎-S

Firebase 配置安全检测

标题	严重程度	描述信息
应用与Firebase数据库通信	信息	该应用与位于 https://criclive-72dee.firebaseio.com 的 Firebase 数据库进行通信
Firebase远程配置已禁用	安全	Firebase远程配置URL （ https://firebaseremoteconfig.googleapis.com/v1/projects/919747867342/namespaces/firebase:fetch?key=AIza5y[redacted]PNzXcg ） 已禁用。响应内容如下所示： 响应码是 403

第三方 SDK 组件分析

SDK名称	开发者	描述信息
Audience Network SDK	Facebook	The Audience Network allows you to monetize your Android apps with Facebook ads. An interstitial ad is a full screen ad that you can show in your app. Typically interstitial ads are shown when there is a transition in your app. For example -- after finishing a level in a game or after loading a story in a news app.
Google Sign-In	Google	提供使用 Google 登录的 API。
Google Play Services	Google	借助 Google Play 服务，您的应用可以利用由 Google 提供的最新功能，例如地图，Google+ 等，并通过 Google Play 商店以 APK 的形式分发自动平台更新。 这样一来，您的用户可以更快地接收更新，并且可以更轻松地集成 Google 必须提供的最新信息。
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。
Jetpack App Startup	Google	App Startup 库提供了一种直接，高效的方法来在应用程序启动时初始化组件。库开发人员和应用程序开发人员都可以使用 App Startup 来简化启动顺序并显式设置初始化顺序。App Startup 允许您定义共享单个内容提供程序的组件初始化程序，而不必为需要初始化的每个组件定义单独的内容提供程序。这可以大大缩短应用启动时间。
Jetpack WorkManager	Google	使用 WorkManager API 可以轻松地调度即使在应用退出或设备重启时仍应运行的可延迟异步任务。
Audience Network	Facebook	通过 Facebook 广告使您通过移动媒体资源获利

Firebase	Google	Firebase 提供了分析、数据库、消息传递和崩溃报告等功能，可助您快速采取行动并专注于您的用户。
Picasso	Square	一个强大的 Android 图片下载缓存库。
Jetpack Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。
Jetpack ProfileInstaller	Google	让库能够提前预填充要由 ART 读取的编译轨迹。
Firebase Analytics	Google	Google Analytics（分析）是一款免费的应用衡量解决方案，可提供关于应用使用情况和用户互动度的分析数据。
Jetpack AppCompat	Google	Allows access to new APIs on older API versions of the platform (many using Material Design).
Jetpack Room	Google	Room 持久性库在 SQLite 的基础上提供了一个抽象层，让用户能够在充分利用 SQLite 的强大功能的同时，获享更强健的数据库访问机制。

邮箱地址敏感信息提取

EMAIL	源码文件
payments.cricketlineguru@gmail.com	com/app/cricketapp/features/premium/subscription/SubscriptionPlansActivity.java
this@createcapturedifneeded.type	tt/d$a.java
feedback.clg@gmail.com	p8/b.java
this@abstracttypeconstructor.builtins this@abstracttypeconstructor.paramete	gu/i$a.java

第三方追踪器检测

名称	类别	网址
Facebook Ads	Advertisement	https://reports.exodus-privacy.eu.org/trackers/65
Facebook Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/66
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
Fyber	Advertisement	https://reports.exodus-privacy.eu.org/trackers/104
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
IAB Open Measurement	Advertisement, Identification	https://reports.exodus-privacy.eu.org/trackers/328
Inmobi		https://reports.exodus-privacy.eu.org/trackers/106

敏感凭证泄露检测

可能的密钥
AdMob广告平台的=> "com.google.android.gms.ads.APPLICATION_ID" : "@string/google_ads_id"
"com.google.firebase.crashlytics.mapping_file_id" : "a13f768f2ffe4d97b38826e598b16e83"
"easypay_password" : "Password"
"facebook_app_id" : "227435798169211"
"firebase_database_url" : "https://criclive-72dee.firebaseio.com"
"google_api_key" : "AIzaSyACaYfgAurCWbz0k1qOlYn3z9eELPNzXcg"
"google_app_id" : "1:919747867342:android:003807c9003db583"
"google_crash_reporting_api_key" : "AIzaSyACaYfgAurCWbz0k1qOlYn3z9eELPNzXcg"
"pass" : "Pass"
O+nZ2lSoRNBpWXwu/ip6DLZjtNsCYqy9HP8i3F1GcCw=
2D24A89831BEFC769DA3E4F16E44C468
43D8ABFACBD6B5E7F28D283713DB88FD
257614FA21C0D26B1AA41D649E8D1BE8
0C25D485EE51FB27F4998E257D391FFC
66F21BA37BCCE5DD9F469402B9C40605
C31916EF794AC19B4EC7000D6522843D
935E451DA5957C04F6839271AB5C2CE0
470fa2b4ae81cd56ecbcda9735803434cec591fa
37FFF62E2EE7A1A03D5362676CED6C68
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
9b8f518b086098de3d77736f9458a3d2f6f95a37
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
922498738D4E8A5D003BF0516BE4397E
81807B3CAB02831C333BC71D9B2F82EC
597d16e892fb3d46a6b5c12ac5b3a112
14BC5A0DDEA1EC7636AC4853F2E6C8CB
c56fb7d591ba6704df047fd98f535372fea00211
5D6CA7D2968C56BC5D8D1DF8922993A1
D2E70FE764F3D27921074C8557AAF20C

16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
4DF0F7FE9D127FFE9A9B9442219EBDCE
Vn3kj4pUbIROi2S+QfRRL9nhsaO2uoHQg6+dpEtxdTE=
cc2751449a350f668590264ed76692694a80308a
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
B5B52DE47A7D6109345D976358BE90C1
31EE96364F11B01DBEE77E9DA784F3E9
26B827DBC5E8E05B47D3424F3FE58E8B
0000016742C00BDA259000000168CE0F13200000016588840DCE7118A0002FBF1C31C3275D78
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
1A7A9667CD2FDCD539D11E0BA7D51904
D84959E9DFC86D842079CAB31859C5A4
4014633F4F00A24515B2667FCEAAC942
bd5def51f4c9cdfcae0bc85addb1acfe
1C506DB08BC0F72B4412E77A7D8554F2

Google Play 应用市场信息

标题: Cricket Line Guru

评分: 4.498293 **安装:** 50,000,000+ **价格:** 0 **Android版本支持:** **分类:** 体育 **Play Store URL:** com.app.cricketapp

开发者信息: Cricket Line Guru, Cricket+Line+Guru, DELHI, INDIA, https://cricketlineguru.com, cricketlineguruapp@gmail.com,

发布日期: 2017年5月5日 **隐私政策:** Privacy link

关于此应用:

Cricket Line Guru 致力于为您提供每场板球比赛的最佳实时板球比分更新以及： - 现场逐球解说 - 详细的记分卡 - 场地详情 - 出场阵容和阵容 - 引脚分数 - 热门新闻和故事 - 即将举行的系列赛和比赛详情 - 进行民意调查并查看其他人的意见 - 实时和即将举行的比赛的警报和通知。 - 准确的比赛赔率和场次。 - 排名、统计数据和记录。 - 所有板球场地的列表以及每个运动员的详细信息。 即时板球比赛更新、板球直播比分、直播板球比赛、评论、新闻、民意调查和赛程、直播 IPL 比赛、直播比赛、关注所有巡回赛和奖杯的现场板球比分。 例如印度超级联赛、T20 世界杯、ODI 世界杯、测试锦标赛、冠军奖杯和国际巡回赛。 除此之外，我们还覆盖所有英超和国内联赛，如世界杯、印度超级联赛（IPL）、Big Bash Tournament（BBL）、巴基斯坦T20联赛（PSL）、加勒比T20联赛（CPL）、孟加拉国T20联赛（ BPL）、阿布扎比 T10 联赛、T20 Blast、县板球、超级 50 杯、百强赛、女子 Big Bash 联赛、百强女子比赛等。 应用选项卡： 首页 - 多场精选比赛 - 热门系列 - 热门新闻和视频 直播 - 单独的选项卡可轻松访问所有现场比赛 比赛 - 即将举行和最近的比赛 - 分类为全部、T20、ODI、TEST 短裤 - 即时最新板球更新 - 病毒式流行的图片和视频 系列 - 所有热门系列尽在一个屏幕中 - 完整的系列信息和统计数据 - 赛程、积分表、球队、场地、新闻和视频 - 表现最佳的球员 民意调查 - 对您最喜欢的球队进行民意调查 - 查看民意调查的百分比 更多 - 浏览系列 - 浏览团队 - 浏览玩家 - 排名 - 我们的社交媒体 高级版： 您可以订阅我们的高级版本，享受无广告的体验，并享受 Pro Score 和赔率历史记录等其他好处。这是相当合理的，所以请升级并体验最好的板球应用程序，无广告。 下载该应用程序并通过 Cricket Line Guru 应用程序享受板球运动。

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。