南明离火
移动应用检测平台

ANDROID 静态分析报告

放课后的捉迷藏汉化版v5.1 • v01.28.03

分析日期: 2024-08-02 07:44:23

应用概览

文件名称:	92281.apk
文件大小:	18.46MB
应用名称:	放课后的捉迷藏汉化版v5.1
软件包名:	jp.cloverlab.yurudora
主活动:	jp.cloverlab.yurudora.Yurudora
版本号:	01.28.03
最小SDK:	15
目标SDK:	23
加固信息:	未加壳
应用程序安全分数:	45/100 (中风险)
跟踪器检测:	6/432
杀软检测:	3 个杀毒软件报毒
MD5:	a3304d040d463ee3e006f7cda3a98ec1
SHA1:	e15960d9a952cfd259a4ada25[illegible]d9b8c2419
SHA256:	a7780aa1452bcffd0d0b91[illegible]d9320652916adf1779c[illegible]fb7a3bb01b0709b6e1

分析结果严重性分布

高危	危	信息	安全	关注
6	2	2	2	2

四大组件导出状态统计

Activity组件：43个，其中export的有： 2个
Service组件：3个，其中export的有： 1个
Receiver组件：4个，其中export的有： 4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=x, ST=x, L=x, O=x, OU=x, CN=x
签名算法: rsassa_pkcs1v15
有效期自: 2018-12-15 05:25:53+00:00
有效期至: 2043-12-09 05:25:53+00:00
发行人: C=x, ST=x, L=x, O=x, OU=x, CN=x
序列号: 0x5eba007c
哈希算法: sha256
证书MD5: becb01ffcc1734e9977ea8245be258b6
证书SHA1: 553833f1c996e4a22a350698225eaf84b7d1df17
证书SHA256: 2a22927eb969bbf8a0b4e009f9e1f6274029d903b65aa56d4c21e6e4cf426d38
证书SHA512:
41ff8aeeca44c9238c13083579bce09716013568229a557b12c3cc11cfe80f1fe842ceaa9da94d210decebbf3e83bb31b34b8117f9ab0656b0e14c83628fd13f

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。
com.android.vending.BILLING	普通	应用程序具有应用内购买	允许应用程序从 Google Play 进行应用内购买。
jp.cloverlab.yurudora.permission.C2D_MESSAGE	未知	未知权限	来自 android 引用的未知权限。
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。
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.GET_ACCOUNTS	普通	探索已知账号	允许应用程序访问帐户服务中的帐户列表。
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.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.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.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。

可浏览 Activity 组件分析

ACTIVITY	INTENT
jp.cloverlab.yurudora.Yurudora	Schemes: yurudora://, Hosts: app.yuru.cloverlab.biz, top, collabo,
com.kayac.lobi.sdk.activity.RootActivity	Schemes: nakamapapp-bbe5770aceba6a29ee4dd545a84a60111f73783e://,

com.kayac.lobi.sdk.activity.invitation.InvitationActivity	Schemes: nakamap://, Hosts: invited,

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: **0** | 警告: **16** | 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	应用程序数据可以被备份 [android:allowBackup=true]	警告	这个标志允许任何人通过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	Broadcast Receiver (com.google.android.gcm.GCMBroadcastReceiver) 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。
4	Service (com.kayac.nakamap.sdk.auth.NakamapAuthCallbackService) 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。
5	Activity (com.kayac.lobi.sdk.activity.RootActivity) 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	Broadcast Receiver (it.partytrack.sdk.ReferrerReceiver) 未被保护。 [android:exported=true]	警告	发现 Broadcast Receiver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	Broadcast Receiver (jp.cloverlab.yurudora.ReceiverMat) 未被保护。 [android:exported=true]	警告	发现 Broadcast Receiver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设置了TaskAffinity属性 (com.digits.sdk.android.PhoneNumberActivity)	警告	如果设置了 taskAffinity，其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息，请始终使用默认设置，将 affinity 保持为包名
9	Activity设置了TaskAffinity属性 (com.digits.sdk.android.ConfirmationCodeActivity)	警告	如果设置了 taskAffinity，其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息，请始终使用默认设置，将 affinity 保持为包名
10	Activity设置了TaskAffinity属性 (com.digits.sdk.android.LogInCodeActivity)	警告	如果设置了 taskAffinity，其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息，请始终使用默认设置，将 affinity 保持为包名
11	Activity设置了TaskAffinity属性 (com.digits.sdk.android.TwitterLoginActivity)	警告	如果设置了 taskAffinity，其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息，请始终使用默认设置，将 affinity 保持为包名
12	Activity设置了TaskAffinity属性 (com.digits.sdk.android.PhoneNumberActionBarActivity)	警告	如果设置了 taskAffinity，其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息，请始终使用默认设置，将 affinity 保持为包名
13	Activity设置了TaskAffinity属性 (com.digits.sdk.android.ConfirmationCodeActionBarActivity)	警告	如果设置了 taskAffinity，其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息，请始终使用默认设置，将 affinity 保持为包名
14	Activity设置了TaskAffinity属性 (com.digits.sdk.android.LogInCodeActionBarActivity)	警告	如果设置了 taskAffinity，其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息，请始终使用默认设置，将 affinity 保持为包名
15	Activity设置了TaskAffinity属性 (com.digits.sdk.android.TwitterLoginActionBarActivity)	警告	如果设置了 taskAffinity，其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息，请始终使用默认设置，将 affinity 保持为包名
16	Activity (com.kayac.lobi.sdk.activity.invitation.InvitationActivity) 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。
17	Broadcast Receiver (com.kayac.lobi.sdk.receiver.AppInstallReceiver) 未被保护。 [android:exported=true]	警告	发现 Broadcast Receiver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。

本报告由南明离火移动安全分析平台生成

代码安全漏洞检测

高危: **4** | 警告: **8** | 信息: **2** | 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
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	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
4	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
5	不安全的Web视图实现。可能在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
6	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
7	该文件是World Writable。任何应用程序都可以写入文件	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
8	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

9	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
10	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
11	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
12	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-2	升级会员：解锁高级权限
13	SHA-1是已知存在哈希冲突的弱哈希	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
14	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
15	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
16	应用程序使用带PKCS5/PKCS7填充加密模式CBC。此配置易受到填充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

类型	匹配	权限

本报告由南明离火移动安全分析平台生成

恶意软件常用权限	4/30	android.permission.WAKE_LOCK android.permission.GET_ACCOUNTS android.permission.READ_PHONE_STATE android.permission.VIBRATE
其它常用权限	5/46	android.permission.INTERNET com.google.android.c2dm.permission.RECEIVE android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE 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
support.twitter.com	安全	否	**IP地址:** 104.244.42.67 **国家:** 美利坚合众国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.7[illegible]968 **经度:** -122.410446 **查看:** Google 地图
nakamap.com	安全	否	No Geolocation information available.
www.googletagmanager.com	安全	是	**IP地址:** 180.163.151.169 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.224333 **经度:** 121.468948 **查看:** 高德地图
minidumps.smbeat.jp	安全	否	No Geolocation information available.
api-owr-bootstrap-stage.metaps.net	安全	否	No Geolocation information available.
nakamapapps.com	安全	否	No Geolocation information available.
blog.lobi.co	安全	否	No Geolocation information available.
api-owr-bootstrap.metaps.net	安全	否	No Geolocation information available.
api.smbeat.jp	安全	否	No Geolocation information available.
and.noahapps.jp	安全	否	No Geolocation information available.
lobi.co	安全	否	**IP地址:** 13.226.228.101 **国家:** 美利坚合众国 **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

本报告由南明离火移动安全分析平台生成

thanks.lobi.co	安全	否	No Geolocation information available.
goo.gl	安全	否	**IP地址:** 142.250.68.110 **国家:** 美利坚合众国 **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
market.android.com	安全	否	**IP地址:** 142.250.72.238 **国家:** 美利坚合众国 **地区:** 科罗拉多州 **城市:** 丹佛 **纬度:** 39.739361 **经度:** -104.983597 **查看:** Google 地图
api.twitter.com	安全	否	**IP地址:** 104.244.42.66 **国家:** 美利坚合众国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.773968 **经度:** -122.410446 **查看:** Google 地图
twitter.com	安全	否	**IP地址:** 104.244.42.66 **国家:** 美利坚合众国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.773968 **经度:** -122.410446 **查看:** Google 地图
api-owr-bootstrap-dev.metaps.net	安全	否	No Geolocation information available.
images.smbeat.jp	安全	否	No Geolocation information available.
web.lobi.co	安全	否	**IP地址:** 13.226.228.69 **国家:** 美利坚合众国 **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
syndication.twitter.com	安全	否	**IP地址:** 104.244.42.8 **国家:** 美利坚合众国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.773968 **经度:** -122.410446 **查看:** Google 地图
lobi-faq.tdnapp.com	安全	否	**IP地址:** 74.114.154.22 **国家:** 美利坚合众国 **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

e.crashlytics.com	安全	否	No Geolocation information available.
reward-sb.gree.net	安全	否	**IP地址:** 18.176.75.196 **国家:** 日本 **地区:** 东京 **城市:** 东京 **纬度:** 35.689499 **经度:** 139.692322 **查看:** Google 地图
reward.gree.net	安全	否	**IP地址:** 3.112.154.45 **国家:** 日本 **地区:** 东京 **城市:** 东京 **纬度:** 35.689499 **经度:** 139.692322 **查看:** Google 地图
settings.crashlytics.com	安全	否	No Geolocation information available.
control.smbeat.jp	安全	否	No Geolocation information available.
app.yuru.cloverlab.biz	安全	否	**IP地址:** 61.160.145.90 **国家:** 中国 **地区:** 江苏 **城市:** 台州 **纬度:** 32.492168 **经度:** 119.910767 **查看:** 高德地图
www.digits.com	安全	否	**IP地址:** 34.95.92.107 **国家:** 美利坚合众国 **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

URL 链接安全分析

URL信息	源码文件
• https://%s%s/%s?token=%s	com/kayac/lobi/sdk/service/chat/GroupEventPollingTask.java
• http://and.noahapps.jp/api.php	jp/noahapps/sdk/h.java
• http://market.android.com • https://play.google.com	jp/noahapps/sdk/NoahBrowserActivity.java
• http://market.android.com • https://play.google.com	jp/noahapps/sdk/NoahOfferActivity.java
• http://app.yuru.cloverlab.biz/yyy/up_device • http://app.yuru.cloverlab.biz/yyy/down_device	jp/cloverlab/yurudora/b.java
• https://web.lobi.co/user/	com/kayac/lobi/sdk/activity/profile/ProfileActivity.java

• https://lobi.co/sp/store?from=chatsdk&referrer=%s	com/kayac/lobi/sdk/utils/ReferrerUtil.java
• http://blog.lobi.co • http://nakamap.com/page/asct • https://thanks.lobi.co/video/faq.html • http://lobi-faq.tumblr.com/tagged/sdk • http://lobi.co/terms	com/kayac/lobi/sdk/activity/menu/MenuActivity.java
• https://control.smbeat.jp/api/remote	com/smrtbeat/RunnableC0199i.java
• http://reward.gree.net • http://reward-sb.gree.net	net/gree/reward/sdk/a.java
• https://twitter.com/share?text=	net/metaps/sdk/JSController.java
• http://nonbody • javascript:webviewclient.viewsource	org/cocos2dx/lib/gree/webview/Cocos2dxWebView.java
• http://and.noahapps.jp/api.php	jp/noahapps/sdk/q.java
• http://lobi.co/ad/other/sdk?page=%s&platform=%s	com/kayac/lobi/libnakamap/components/AdComponent.java
• https://docs.google.com/spreadsheet/formresponse?formkey=%s&ifq	org/acra/a.java
• https://minidumps.smbeat.jp/api/errors/multi • https://images.smbeat.jp/api/upload • https://api.smbeat.jp/api/errors • https://control.smbeat.jp/api/remote	com/smrtbeat/C0193c.java
• https://docs.google.com/spreadsheet/formresponse?formkey=%s&ifq	org/acra/a/a.java
• https://minidumps.smbeat.jp/api/errors/multi	com/smrtbeat/C0201k.java
• https://minidumps.smbeat.jp/api/errors/multi • https://images.smbeat.jp/api/upload • https://api.smbeat.jp/api/errors • https://control.smbeat.jp/api/remote	com/smrtbeat/C0192b.java
• https://images.smbeat.jp/api/upload	com/smrtbeat/C0204n.java
• https://minidumps.smbeat.jp/api/errors/multi • https://api.smbeat.jp/api/errors	com/smrtbeat/C0195e.java
• https://twitter.com/tos • https://www.digits.com	com/digits/sdk/android/w.java
• http://api-owr-bootstrap.metaps.net/3_0_1.json • http://api-owr-bootstrap-stage.metaps.net/3_0_1.json • http://api-owr-bootstrap-dev.metaps.net/3_0_1.json	net/metaps/sdk/Const.java
• 1.1.0.25	com/digits/sdk/android/t.java
• https://nakamapapps.com	com/kayac/lobi/sdk/net/ProductServerConfig.java

• https://www.googletagmanager.com • http://reward-sb.gree.net • http://hostname/? • http://plus.google.com/ • http://app.yuru.cloverlab.biz/yyy/down_device • http://goo.gl/nafqqk • https://twitter.com/%s/status/%d • http://lobi.co/terms • http://blog.lobi.co • https://syndication.twitter.com • https://api.twitter.com • 1.1.0.25 • http://www.google.com • https://twitter.com/tos • http://api-owr-bootstrap.metaps.net/3_0_1.json • http://reward.gree.net • https://thanks.lobi.co/video/faq.html • http://lobi-faq.tumblr.com/tagged/sdk • https://twitter.com/%1$s/status/%2$s • https://minidumps.smbeat.jp/api/errors/multi • https://play.google.com • http://api-owr-bootstrap-dev.metaps.net/3_0_1.json • https://web.lobi.co/user/ • 1.1.1.25 • https://nakamapapps.com • http://nakamap.com/page/asct • https://www.digits.com • https://support.twitter.com/forms/platform • http://app.yuru.cloverlab.biz/yyy/up_device • https://api.smbeat.jp/api/errors • https://images.smbeat.jp/api/upload • 1.0.3.25 • https://settings.crashlytics.com/spi/v2/platforms/android/apps/%s/settings • https://control.smbeat.jp/api/remote • https://twitter.com/? • http://market.android.com • http://lobi.co/ad/other/sdk?page=%s&platform=%s • https://twitter.com/share?text= • http://nonbody • https://docs.google.com/spreadsheet/formResponse?formkey=%s&ifq • http://api-owr-bootstrap-stage.metaps.net/3_0_1.json • https://e.crashlytics.com/spi/v2/events • http://and.noahapps.jp/api.php • https://%s%s/%s?token=%s • https://lobi.co/sp/store?from=matsdk&referrer=%s • javascript:webviewClient.viewsource	自研引擎-S

第三方 SDK 组件分析

SDK名称	开发者	描述信息
cocos2d-cpp	cocos2d-cpp	cocos2d-cpp 是用 C++ 14 编写的 2D 便携式游戏引擎，适用于 Android，iOS，Linux，MacOS 和 Windows。
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
info@lobi.co	com/kayac/lobi/sdk/activity/menu/MenuActivity.java
cs_yurudora@cloverlab.jp	jp/cloverlab/yurudora/YurudoraApplication.java
your.account@domain.com	org/acra/ErrorReporter.java
info@lobi.co cs_yurudora@cloverlab.jp your.account@domain.com	自研引擎-S

第三方追踪器检测

名称	类别	网址
ACRA	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/444
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Tag Manager	Analytics	https://reports.exodus-privacy.eu.org/trackers/105
Tune	Analytics	https://reports.exodus-privacy.eu.org/trackers/38

敏感凭证泄露检测

可能的密钥
凭证信息=> "com.crashlytics.ApiKey" : "c56da0b3bc34325482ff49940b0d752c30ad9ec6"
"lobi_private_groups" : "Private"
"lobi_visibility_private" : "PRIVATE"
"lobi_visibility_private" : "PRIVATE"
bbc23e290bb3287fdad3ea24dbdf423bd06b03d
b01989e7effb4aafcb148f58463976214150c1ba
5519b278acb281d7eda7abc18399b3bb690424b5
c07a98688d89fbab05640c117daa7d65b8cacc4e

3082025d308201c6a00302010202044bd76cce300d06092a864886f70d01010505003073310b30090603550406130255533 10b30090603550408130243413116301406035504070d53616e204672616e636973636f3116301406035504a130d547769747465722c20496e632e310f300d060355040b13064d6f62696c653116301406035504031 30d4c656c616e642052656368697330 1e170d313030343237323330313334 5a170d3438303832353233303313334 5a3073310b30090603550406130255533 10b30090603550408130243413116301406035504070d53616e204672616e636973636f3116301406035504a130d547769747465722c20496e632e310f300d060355040b13064d6f62696c653116301406035504031 30d4c656c616e6420526563686973697 330819f300d06092a864886f70d010101050003818d00308189028181008623 3c2e51c62232d49cc932e470713d63a6a1106b38f9e442e01bc79ca4f95c72b2cb3f1369ef7dea6036bff7c4b2828cb3787e7657ad83986751ced5b131fcc6f413efb7334e32ed9787f9e9a249ae108fa66009ac7a7932c25d37e1e07d4f9f66aa494c270dbac87d261c9668d321c2fba4ef2800e46671a597ff2eac5d7f0203010001300d06092a864886f70d01010505000381810 03e1f01cb6ea8be8d2cecef5cd2a64c97ba8728aa5f08f8275d00508d64d139b6a72c5716b40a040df0eeeda04de9361107e123ee8d3dc05e70c8a355f46dbadf1235443b0b214c57211afd4edd147451c443d49498d2a7ff27e45a99c39b9e47429a1dae843ba233bf8ca81296dbe1dc5c5434514d995b0279246809392a219b
5abec575dcaef3b08e271943fc7f250c3df661e3
e27f7bd877d5df9e0a3f9eb4cb0e2ea9efdb6977
1237ba4517eead2926fdc1cdfebeedf2ded9145c
40a8eefe-2489-4b5d-bf28-1da84b1e41ba
22f19e2ec6eaccfc5d2346f4c2e8f6c554dd5e07
1a21b4952b6293ce18b365ec9c0e934cb381e6d4
bdbea71bab7157f9e475d954d2b727801a822682
3c03436868951cf3692ab8b426daba8fe922e5bd
83317e62854253d6d7783190ec919056e991b9e3
713836f2023153472b6eba6546a9101558200509
d52e13c1abe349dae8b49594ef7c3843606466bd
9ca98d00af740ddd8180d21345a58b8f2e9438d6
b181081a19a4c0941ffae89528c124c99b34a[illegible]
4d0ZDlQNWABqMLDtLeqV5jZrd8viyK[illegible]XA5fFFY8Hmvrlbuf
ed663135d31bd4eca614c429e3[illegible]94c12650
2343d148a255899b947d461a[illegible]c04cfed170b7
070e24cd-34bb-4[illegible]e8ac8fe55a10
56fef3c2147d4e[illegible]fdbd3052387201e57738d
87e85b6353c623a3128cb0ffbbf551fe[illegible]e22
68330e61358521592983a3c8[illegible]1406e7ab3c1
5e4f538685dd4f9[illegible]56f7d51b1dc9b7b

308201e730820150a00302010202044cd7f274300d06092a864886f70d01010505003037310e300c060355040a13054b41594143310c300a060355040b1303496e6331173015060355040403130e5461726f204b6f6261796173686930819f300d06092a864886f70d010101050003818d00308189028181009209f3b882abe7f9a145ec63acbcb86dee40e15f14328b6593e98b50aa544346d918af03a401b248fd7a94f980c934636fe0f08ace7bfc9b8584bbbcf58c8056b51c17d06d77b0145674b0693a2c928e325e775cd62d5aff1eba0b908c4db0e86b99967a4238c97add47a439360889e24c01cdae2343d36d9698f634f913bad0203010001300d06092a864886f70d0101050500038181007147f2bc328634ecff20476c4cba572958b09099da4d82d6dc20aa4869bbca7fccf8231fb092c24457a2d8a16c75020984fbade9d7eea59be6a9bfdf39926e12670ecde475ec6b2cc6ac0ace84558a455a3b8f3801e1d86928bc3cb2f2b79d6d869cbe85598c8f9c11b8a63e4d9d05d93861bf780a14268c50e5629c32abe921

Google Play 应用市场信息

标题: ゆるドラシル-本格派RPG- バトってボケて世界を救え

评分: 4.017903 **安装:** 1,000,000+ **价格:** 0 **Android版本支持:** **分类:** 角色扮演 **Play Store URL:** jp.cloverlab.yurudora

开发者信息: cloverlab.inc, cloverlab.inc, 大阪府大阪市北区豊崎 5 丁目 6 − 2 , http://yurudora.com/, cs_yurudora@cloverlab.jp,

发布日期: None **隐私政策:** Privacy link

关于此应用:

◆您无需重新安排流程即可开始！ ◆ ◆恭喜！ 10周年纪念日！ ◆ ◆下载量超过700万次！ ◆ // 无需重新滚动 // 您可以多次重画第一个扭蛋，无需重新滚动！ 继续努力，直到赢得你最喜欢的角色！ // 特别奖励 // 初学者必看！我们目前正在提供特别奖励，您可以获得超级强大的单位和奢侈品！ 连续登录7天，即可获得2张“女武神兑换券”，可以选择自己喜欢的战女兵种！ 1个特殊物品套装”，包含超过 40 件物品！ 而且你一定会获得“终极觉醒特别兑换券”，可以选择超强的终极觉醒单位！ 此外，我们正在举办初学者活动！ 您可以获得总共 19,000 个金币，可用于 5 天的扭蛋！ 现在是开始的时候了！ ！ // 疯狂起来，拯救世界！ // 一款以严肃而滑稽的故事展开的神话角色扮演游戏现已推出！ 我从来没有见过这样的神话！ 以宏大的神话世界为背景，可爱的角色横冲直撞！ ！ 正宗RPG配备命令选择战斗！ ！ 《Yurudora》的三大特点 ① 通过命令输入进行简单的自动进度战斗，增加深度！简单又刺激的战斗，还有许多华丽的必杀技！ ！ ② 宽松又流行的角色，让人产生共鸣！ 神话中的诸神、英雄、甚至敌人的巨人都以滑稽而独特的角色的形式出现！ ！ ③ 仅仅可爱是不够的！以神话世界为背景，可爱的角色创造了一个时而滑稽、时而严肃的史诗故事！ // 命令输入式自动战斗系统 // 战斗是命令输入式的自动战斗，关键是根据实时变化的战况来选择命令！ 从华丽的魔法到必杀技、恢复、状态异常……简单轻松的元素让您享受RPG迷无法抗拒的刺激战斗！ 使用为每个角色准备的各种命令来对抗神话世界中的强大敌人！ // 故事 // 在诸神居住之地瓦尔哈拉，“耳朵基里”是众女神中最受欢迎的祭司，直属主神奥丁麾下。 成为女武神一员的主角，前往主神奥丁那里接受第一个任务。 当我们看到他紧张、还有一些不安时，下一个等待着我的是什么…… 为了面对预言中的末日之战“诸神黄昏”，在主神奥丁的指挥下，你将与托尔等挪威神话中熟悉的神灵一起探索与世界树“Yggdrasil”相连的广阔世界、芙蕾雅和洛基。 主角们能否改变毁灭的命运呢？ ？ 请欣赏独特的神灵讲述的宽松而又史诗般的故事！ // 为故事增添色彩的人物 // ◇主神奥丁 众神之首。 他曾经是一个统领万神的神奇大神，不知不觉间，他变成了一个混蛋，他最新的口头禅是“我不想工作”。 他非常健忘、笨拙，并且给出的指令非常随意。 我拥有 5 件我最喜欢的奥登 T 恤，包括备用件。 ◇雷神托尔 善良又坚强！虽然他经常和奥丁一起在天界玩耍，但他却是个猛人，在众神的战争中担任过特攻小队的指挥官。 他没有思想，认为大多数事情都可以通过肌肉来解决。 她极其不擅长使用武力，整天破坏神殿里的物品和贵重文物，结果却遭到芙蕾雅的责罚。 他很喜欢上面写着“Toru”字样的海面包，这是他女儿送给他的礼物。 ◇生育女神芙蕾雅 他是天上最有常识的人。 因此，他总是对奥丁和托尔的行为做出严厉但准确的评论。 她对后辈和新人很友善，并善意地支持主角新女武神。 ◇圣兽斯雷普尼尔 原本以奥丁之马而闻名的神兽。 一次偶然的机会，他变成了人形，但与他令人印象深刻的外表相反，他以绅士闻名。 为了履行作为人类形态的骑士的职责，最近他将奥丁背在肩上，或者放在公主的怀里前往目的地。

免责声明及风险提示: