南明离火
移动应用检测平台

ANDROID 静态分析报告

□□ • v1.0.15

分析日期: 2025-03-11 11:10:10

i应用概览

文件名称:	i-i-pumss-v1015.apk
文件大小:	3.77MB
应用名称:	□□
软件包名:	com.bitran.gatown
主活动:	com.bitran.gatown.MainActivity
版本号:	1.0.15
最小SDK:	24
目标SDK:	33
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	56/100 (中风险)
跟踪器检测:	1/432
杀软检测:	经检测，该文件安全
MD5:	deb49cf7c9f17b0e46ce5191613f4be1
SHA1:	c0cc4652155251c0bff38ecbd47d06bb4c637c91
SHA256:	c5dd2029f735b32804374c6b19242e57aa67e3dd2866b2a861f119d35107e87b

分析结果严重性

高危	中危	信息	安全	关注
0	10	3	1	0

四大组件信息

Activity组件：3个，其中export的有：0个
Service组件：10个，其中export的有：3个
Receiver组件：11个，其中export的有：3个
Provider组件：2个，其中export的有：0个

证书信息

二进制文件已签名
v1 签名: False
v2 签名: True
v3 签名: False
v4 签名: False
主题: C=KR, ST=Seoul, L=Gengnam, O=bitran, OU=bitran, CN=bitran
签名算法: rsassa_pkcs1v15
有效期自: 2019-11-26 05:54:55+00:00
有效期至: 2044-11-19 05:54:55+00:00
发行人: C=KR, ST=Seoul, L=Gengnam, O=bitran, OU=bitran, CN=bitran
序列号: 0x4492a7bb
哈希算法: sha256
证书MD5: 17a4aaffb78a33fd022f599f4ad93241
证书SHA1: 70f4f0edf5260cd97f9687635d11922aa0145291
证书SHA256: 5e04882d347e1c2ec81b3c9d874214a37582d26473aae6232f567edc51f83043
证书SHA512:
ce40dfdfdbd893539f17d6156afa53d9d2be0bb199ace66301a1e1b782abed1eb5b5f7706c35e735ff31e8c30af7497bbbb7[illegible]eb519ac938343e14abe5b66dd5

公钥算法: rsa
密钥长度: 2048
指纹: 58bbefa9bbbc46053bf8bfc8c158d8e02cde592861f60c611b3ea8604c036e90
找到 1 个唯一证书

应用权限

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.READ_EXTERNAL_STORAGE	危险	读取SD卡内容	允许应用程序从SD卡读取信息。
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.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.READ_CONTACTS	危险	读取联系人信息	允允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可借此将您的数据发送给其他人。
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.CAMERA	危险	拍照和录制视频	允许应用程序拍摄照片和视频，且允许应用程序收集相机在任何时候拍到的图像。
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。
com.sec.android.provider.badge.permission.READ	普通	在应用程序上显示通知计数	在三星手机的应用程序启动图标上显示通知计数或徽章。
com.sec.android.provider.badge.permission.WRITE	普通	在应用程序上显示通知计数	在三星手机的应用程序启动图标上显示通知计数或徽章。
com.htc.launcher.permission.READ_SETTINGS	普通	在应用程序上显示通知计数	在HTC手机的应用程序启动图标上显示通知计数或徽章。
com.htc.launcher.permission.UPDATE_SHORTCUT	普通	在应用程序上显示通知计数	在HTC手机的应用程序启动图标上显示通知计数或徽章。
com.sonyericsson.home.permission.BROADCAST_BADGE	普通	在应用程序上显示通知计数	在索尼手机的应用程序启动图标上显示通知计数或徽章。

com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	普通	在应用程序上显示通知计数	在索尼手机的应用程序启动图标上显示通知计数或徽章。
com.anddoes.launcher.permission.UPDATE_COUNT	普通	在应用程序上显示通知计数	在apex的应用程序启动图标上显示通知计数或徽章。
com.majeur.launcher.permission.UPDATE_BADGE	普通	在应用程序上显示通知计数	在solid的应用程序启动图标上显示通知计数或徽章。
com.huawei.android.launcher.permission.CHANGE_BADGE	普通	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
com.huawei.android.launcher.permission.READ_SETTINGS	普通	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
com.huawei.android.launcher.permission.WRITE_SETTINGS	普通	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
android.permission.READ_APP_BADGE	普通	显示应用程序通知	允许应用程序显示应用程序图标徽章。
com.oppo.launcher.permission.READ_SETTINGS	普通	在应用程序上显示通知计数	在OPPO手机的应用程序启动图标上显示通知计数或徽章。
com.oppo.launcher.permission.WRITE_SETTINGS	普通	在应用程序上显示通知计数	在OPPO手机的应用程序启动图标上显示通知计数或徽章。
me.everything.badger.permission.BADGE_COUNT_READ	未知	未知权限	来自 android 引用的未知权限。
me.everything.badger.permission.BADGE_COUNT_WRITE	未知	未知权限	来自 android 引用的未知权限。
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.RECEIVE_BOOT_COMPLETED	普通	开机自启	允许应用程序在系统完成启动后即自行启动。这样会延长手机的启动时间，而且如果应用程序一直运行，会降低手机的整体速度。
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）
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.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.bitran.gatown.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。

可浏览的Activity组件

ACTIVITY	INTENT
com.bitran.gatown.MainActivity	Schemes: gatown://, Hosts: gatown,

网络通信安全

序号	范围	严重级别	描述

证书安全分析

高危: **0** | 警告: **0** | 信息: **1**

标题	严重程度	描述信息
已签名应用	信息	应用程序使用代码签名证书进行签名

MANIFEST分析

高危: **0** | 警告: **6** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	Service (com.google.firebase.messaging.FirebaseMessagingService) 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。
2	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。
3	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。
4	Broadcast Receiver (com.google.android.gms.measurement.AppMeasurementInstallReferrerReceiver) 受权限保护，但是应该检查权限的保护级别。 Permission: android.permission.INSTALL_PACKAGES [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。
5	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。

6	Service (com.google.firebase.iid.FirebaseInstanceIdService) 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。

安全漏洞检测

高危: **0** | 警告: **2** | 信息: **2** | 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	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
3	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
4	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

行为分析

编号	行为	标签	文件
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
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
00036	从/res/raw目录获取资源文件	反射	升级会员：解锁高级权限
00123	连接到远程服务器后将响应保存为 JSON	网络 命令	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
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
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
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

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
00023	从当前应用程序启动另一个应用程序	反射 控制	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
00192	获取短信收件箱中的消息	短信	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
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
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
00091	从广播中检索数据	信息收集	升级会员：解锁高级权限
00009	将游标中的数据放入JSON对象	文件	升级会员：解锁高级权限
00104	检查给定路径是否是目录	文件	升级会员：解锁高级权限

敏感权限分析

类型	匹配	权限
恶意软件常用权限	5/30	android.permission.VIBRATE android.permission.READ_CONTACTS android.permission.CAMERA android.permission.WAKE_LOCK android.permission.RECEIVE_BOOT_COMPLETED
其它常用权限	7/46	android.permission.INTERNET android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE android.permission.FOREGROUND_SERVICE com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE com.google.android.c2dm.permission.RECEIVE

常用: 已知恶意软件经常滥用的权限。

其它常用权限: 已知恶意软件经常滥用的权限。

域名检测

域名	状态	中国境内	位置信息

m.ahnlab.com	安全	否	**IP地址:** 211.233.80.200 **国家:** 大韩民国 **地区:** 首尔teukbyeolsi **城市:** 首尔 **纬度:** 37.566311 **经度:** 126.977203 **查看:** Google 地图
market.android.com	安全	否	**IP地址:** 142.250.72.174 **国家:** 美国 **地区:** 科罗拉多州 **城市:** 丹佛 **纬度:** 39.739361 **经度:** -104.983507 **查看:** Google 地图
mobile.vpay.co.kr	安全	否	**IP地址:** 203.233.100.54 **国家:** 大韩民国 **地区:** 世宗 **城市:** 世宗 **纬度:** 36.487003 **经度:** 127.282234 **查看:** Google 地图
www.pumss.co.kr	安全	否	**IP地址:** 211.34.105.55 **国家:** 大韩民国 **地区:** 京畿道 **城市:** 城南市 **纬度:** 37.420624 **经度:** 127.126717 **查看:** Google 地图
gatown.firebaseio.com	安全	否	**IP地址:** 35.201.97.85 **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

URL链接分析

URL信息	源码文件
• https://m.ahnlab.com/kr/site/download • https://www.pumss.co.kr/fcpush/fcgetregid.do • https://www.pumss.co.kr/join/syncall.do • https://www.pumss.co.kr • https://mobile.vpay.co.kr/jsp/misp/android.jsp • https://market.android.com	com/bitran/gatown/MainActivity.java
• https://gatown.firebaseio.com	自研引擎-S

FIREBASE数据库分析

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://gatown.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/278848810285/namespaces/firebase:fetch?key=AIzaSyAaOwsaOn_zD8BgK_Z2I4P5hZK4zrvLlzE） 已禁用。响应内容如下所示：
		
		{
		"state": "NO_TEMPLATE"
		}

第三方SDK

SDK名称	开发者	描述信息
Google Play Service	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。
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。
Jetpack Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。
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。

追踪器

名称	类别	网址
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

密钥凭证

可能的密钥
"firebase_database_url" : "https://gatown.firebaseio.com"
"google_api_key" : "AIzaSyAaOwsaOn_zD8BgK_Z2I4P5hZK4zrvLlzE"
"google_app_id" : "1:278848810285:android:371d56e6e8e648a84177a4"
"google_crash_reporting_api_key" : "AIzaSyAaOwsaOn_zD8BgK_Z2I4P5hZK4zrvLlzE"

GooglePlay应用信息

标题: □□ PUMSS

评分: 4.5 **安装:** 10,000+ **价格:** 0 **Android版本支持:** **分类:** 办公 **Play Store URL:** com.bitran.gatown

开发者信息: □□□□□□, %EC%97%94%EC%94%A8%EC%97%98%ED%94%BC%ED%94%8C%EC%8A%A4, None, http://m.ncl.co.kr/NMain/NMain.do, bigused01@ncl.co.kr,

发布日期: 2019年12月8日 **隐私政策:** Privacy link

关于此应用:

我们赢得了客户的心。 （以人为本的非接触式营销支持服务） 即使在移动和数字时代，最终最重要的价值还是人。 Pooms 专注于连接今天的我和明天的我的增长服务。 Pooms 考虑人们会面的交流内容。 Pooms 提出了一个连接公司和客户的成功业务。 “PUMSS”将成为个人、销售人员和公司的“成长阶梯”。 Untact时代营销必备APP！ 支持个人和公司的非面对面销售活动 体验 Pooms 准备的成长、沟通和成功故事。 1. 我的区域（成长） □ 名片 我们将为您制作一张世界上唯一的名片。除了提供基本的名片外，我还通过名片店、设计名片、线下名片等差异化和独特的功能和设计来表达和推广自己。 □ 网络 它配备了对忙碌的现代人有用的群组管理系统。 □ 时间表 您可以轻松管理重大事件和日程安排，例如日、周和月。 □ 日常生活 我诚实地记录了我在忙碌的一天中容易错过的想法和情绪。 2.发送□（通讯） □ 分享 它与包含故事的各种类型的内容进行通信，例如视频、卡片新闻、动画和文本。 □ 每天 没有更多重复和无聊的内容。我们每天都会遇到各种新内容。 □ 信息 我们根据多样化和客观的数据，以易于阅读、有用的方式处理和生产现代人的思想和趋势。 □ 季节 它捕捉了四个季节、季节、纪念日、天气和季节、温度和风力强度。 □ 情绪 从喜讯到艰难时刻，我们不会错过我们的心。 3.渠道（成功） □ 专注 它提供移动销售活动所需的一切，如内容、服务、系统、管理和统计。 □ 资源 您可以方便地为产品、教育、宣传、公告、营销、公司和品牌提供各种材料，并轻松分发给组织和会员。 □ 统计 提供个人和组织以及各种活动和历史作为统计数据。 □ 联锁 可与公司内外部系统灵活对接。 □ 其他 我们以韩国最低的价格免费提供移动礼券、购物中心和算命等销售活动所必需的附加服务。 电子名片、客户管理、日程管理。日记、报价、内容、文字、事件、产品资料、教材、视频资料、礼品展示、商场、算命、组织管理、绩效管理、销售管理、统计管理、推送、会员、群发、积分、等等

免责声明及风险提示: