南明离火
移动应用检测平台

ANDROID 静态分析报告

GUGGISBERG

Guggisberg • v1.25.8

分析日期: 2025-07-07 09:20:59

应用概览

文件名称:	Guggisberg v1.25.8.apk
文件大小:	4.77MB
应用名称:	Guggisberg
软件包名:	ch.involve.app.guggisberg
主活动:	ch.involve.app.guggisberg.MainActivity
版本号:	1.25.8
最小SDK:	28
目标SDK:	34
加固信息:	未加壳
开发框架:	Cordova
应用程序安全分数:	80/100 (低风险)
杀软检测:	经检测，该文件安全
MD5:	276a61f0f5b9c8258f7c67489efad762
SHA1:	9a1a9e442c4d6779d64ca610b543b7860ecbf591
SHA256:	c5aac03c265b27e57c8a9a26fac4f41377c841cf51d010d5d2edcd4d130ae95

分析结果严重性分布

高危	中危	信息	安全	关注
0	4	1	3	0

四大组件导出状态统计

Activity组件：2个，其中export的有： 0个
Service组件：0个，其中export的有： 0个
Receiver组件：2个，其中export的有： 1个
Provider组件：4个，其中export的有： 0个

应用签名证书信息

APK已签名
v1 签名: False
v2 签名: False
v3 签名: True
v4 签名: False
主题: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
签名算法: rsassa_pkcs1v15
有效期自: 2021-09-10 10:54:53+00:00
有效期至: 2051-09-10 10:54:53+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0x815170631529ee19a8bcd4a4eb6e6c241596f6ad
哈希算法: sha256
证书MD5: 9978efbb9602e8e15d3e2a87ddf5d520
证书SHA1: eda98ba067eeb2bfc9ca809858984b710bca7553
证书SHA256: 08079872688759a256f8af5f6fe6b6a88ac824093787db3a4d9a895736120329
证书SHA512:
d23c8934661287f5af82550864afadad7c2ccd2a61466234b38b03c2b38e40923492e29e5c5f3c4d8d71542ae32351bbc0f5f576af9e4[illegible]e9fe95f609956a2

公钥算法: rsa
密钥长度: 4096
指纹: 21ac78937d42e2ec3ebd15f42c0e18b9e9b19c131c78e8d2b8d7ada3b8f50947
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
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.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.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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
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_MEDIA_IMAGES	危险	允许从外部存储读取图像文件	允许应用程序从外部存储读取图像文件。
android.permission.READ_MEDIA_VIDEO	危险	允许从外部存储读取视频文件	允许应用程序从外部存储读取视频文件。
android.permission.READ_MEDIA_AUDIO	危险	允许从外部存储读取音频文件	允许应用程序从外部存储读取音频文件。
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。
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.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.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。

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: **0** | 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: **0** | 警告: **2** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用数据存在泄露风险 未设置[android:allowBackup]标志	警告	建议将 [android:allowBackup] 显式设置为 false。默认值为 true，允许通过 adb 工具备份应用数据，存在数据泄露风险。
2	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) 受权限保护，但应检查权限保护级别。 Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。

代码安全漏洞检测

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

应用行为分析

编号	行为	标签	文件
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
00013	读取文件并将其放入流中	文件	升级会员：解锁高级权限
00072	将 HTTP 输入流写入文件	命令 网络 文件	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
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
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
00191	获取短信收件箱中的消息	短信	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
00175	获取通知管理器并取消通知	通知	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	3/30	android.permission.RECORD_AUDIO android.permission.MODIFY_AUDIO_SETTINGS android.permission.WAKE_LOCK
其它常用权限	9/46	android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.READ_MEDIA_IMAGES android.permission.READ_MEDIA_VIDEO android.permission.READ_MEDIA_AUDIO android.permission.ACCESS_NETWORK_STATE com.google.android.c2dm.permission.RECEIVE

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。

URL 链接安全分析

URL信息	源码文件
• https://github.com/joyent/node/issues/1707 • https://stackoverflow.com/questions/9208814/validate-ipv4-ipv6-and-hostname • https://registry.npmjs.org/tough-cookie/-/tough-cookie-2.4.3.tgz • http://www.iana.org/assignments/character-sets • https://angular.io/license • https://github.com/salesforce/tough-cookie • http://tools.ietf.org/html/rfc3492 • https://fengyuanchen.github.io/cropperjsn • https://mths.be/punycode • https://github.com/ChromiumWebApps/chromium/blob/b3d3b4da8bb94c1b2e061600df106d590fda3620/net/cookies/parsed_cookie.cc • https://tools.ietf.org/html/rfc3492 • https://github.com/exponentjs/tough-cookie-web-storage-store • https://github.com/ChromiumWebApps/chromium/blob/b3d3b4da8bb94c1b2e061600df106d590fda3620/net/cookies/canonical_cookie.cc • https://www.involve.ch • https://www.involve.ch/post/inhalte-mit-der-involve-app-formatieren • http://foo.com • https://github.com/salesforce/tough-cookie/issues • https://www.involve.ch/mettre-en-forme-le-contenu • https://guggisberg-bern.app.involve.ch/api/v1 • https://mathiasbynens.be/notes/javascript-encoding • https://g.co/ng/security • https://github.com/silkimen/cordova-plugin-advanced-http/wiki/Web-APIs-required-for-Multipart-requests • http://jsperf.com/b64tests • http://brianleroux.github.com/lawnchair • https://guggisberg-bern.app.involve.ch/provider/oauth	自研引擎-A

Firebase 配置安全检测

标题	严重程度	描述信息

Firebase远程配置已禁用	安全	Firebase远程配置URL （ https://firebaseremoteconfig.googleapis.com/v1/projects/1998528428733/namespaces/firebase:fetch?key=AIzaSyAZ5w_oSUQEjLtoOWSt6v8OoJoBrJClij8 ） 已禁用。响应内容如下所示：
		
		{
		"state": "NO_TEMPLATE"
		}

第三方 SDK 组件分析

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。
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。

敏感凭证泄露检测

可能的密钥
"google_api_key" : "AIzaSyAZ5w_oSUQEjLtoOWSt6v8OoJoBrJClij8"
"google_app_id" : "1:199852842873:android:7230eecd5ee9c6b8a959a8"
"google_crash_reporting_api_key" : "AIzaSyAZ5w_oSUQEjLtoOWSt6v8OoJoBrJClij8"

Google Play 应用市场信息

标题: Guggisberg

评分: None **安装:** 50+ **价格:** 0 **Android版本支持:** **分类:** 通讯 **Play Store URL:** ch.involve.app.guggisberg

开发者信息: Involve AG, Involve+AG, None, https://www.involve.ch, technologie@involve.ch,

发布日期: None **隐私政策:** Privacy link

关于此应用:

随时随地了解有关贵公司的最新信息，在通讯录中找到您的同事并进行 1:1 聊天或群聊。在安全的瑞士服务器上提供可靠的瑞士软件的一切。 注册也可以在没有电子邮件地址的情况下进行，并有助引导您到您公司的公司信息。只需使用您从公司收到的用户名和密码进行注册。 感谢您使用 Guggisberg 应用程序，我们希望您喜欢它。如果您喜欢该应用程序，我们期待您在 App Store 中发表评论。

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。