南明离火
移动应用检测平台

ANDROID 静态分析报告

OneID • v2.2.5

分析日期: 2025-08-29 05:47:33

应用概览

文件名称:	OneID v2.2.5.apk
文件大小:	21.56MB
应用名称:	OneID
软件包名:	de.wurm.android.oneid
主活动:	de.wurm.android.oneid.SplashscreenActivity
版本号:	2.2.5
最小SDK:	28
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:	65/100 (低风险)
杀软检测:	经检测，该文件安全
MD5:	2e6f5e5ce39e340484065eda1eafcde3
SHA1:	e532824893b2812d6b0ca0fa5cd57ddc99cb4cde
SHA256:	da38cc395ec3e3250095d3a25ff4d35ede4528e2b55f9e70181a53e13d215964

分析结果严重性分布

高危	中危	信息	安全	关注
0	7	2	2	0

四大组件导出状态统计

Activity组件：10个，其中export的有： 0个
Service组件：6个，其中export的有： 0个
Receiver组件：8个，其中export的有： 4个
Provider组件：5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=DE, ST=Germany, L=Remscheid, O=Wurm GmbH & Co. KG, OU=Software Dept., CN=Frank Weller
签名算法: rsassa_pkcs1v15
有效期自: 2013-10-22 07:57:18+00:00
有效期至: 2053-10-12 07:57:18+00:00
发行人: C=DE, ST=Germany, L=Remscheid, O=Wurm GmbH & Co. KG, OU=Software Dept., CN=Frank Weller
序列号: 0x5cde92f5
哈希算法: sha256
证书MD5: fb3155acb2c731007f4fd00c23348acb
证书SHA1: 0dd1beb530793afa315671ff0e5fad9e7c05dffc
证书SHA256: 8d1263a1f1738e218a1566b21d1579f239328ac40d1aa4701bd3f8583052efd4
证书SHA512:
b5006617bd6ad8b42eea98b19040a11c6144559008a3e7f1f66fbb5f909df8fd892377cc85d99a40e00a7635c5c6374a430c9963195f0b2922ff31f5dd3585d9

公钥算法: rsa
密钥长度: 2048
指纹: 6544788c19967d00bf195473f8d0d060fe617b058dfab349b38befadc5b72890
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.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.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.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.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.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。
de.wurm.android.oneid.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
android.permission.USE_BIOMETRIC	普通	使用生物识别	允许应用使用设备支持的生物识别方式。
android.permission.USE_FINGERPRINT	普通	允许使用指纹	此常量在 API 级别 28 中已弃用。应用程序应改为请求USE_BIOMETRIC

可浏览 Activity 组件分析

ACTIVITY	INTENT
de.wurm.android.oneid.SplashscreenActivity	Schemes: wurmoneid://, Hosts: login,

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: **5** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用数据允许备份 [android:allowBackup=true]	警告	该标志允许通过 adb 工具备份应用数据。启用 USB 调试的用户可直接复制应用数据，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。
3	Broadcast Receiver (crc6447fe245e9e46b330.LoginReceiver) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
4	Broadcast Receiver (crc649b9f9e15de895143.DefaultReceiver) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。

本报告由南明离火移动安全分析平台生成

5	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 受权限保护，但应检查权限保护级别。 Permission: android.permission.DUMP [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: **0** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	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
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

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.VIBRATE android.permission.GET_ACCOUNTS android.permission.WAKE_LOCK
其它常用权限	3/46	android.permission.ACCESS_NETWORK_STATE android.permission.INTERNET 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。

恶意域名威胁检测

域名	状态	中国境内	位置信息
fcmpushnotifications-1566b.firebaseio.com	安全	否	**IP地址:** 35.190.39.113 **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 链接安全分析

URL信息	源码文件
• https://fcmpushnotifications-1566b.firebaseio.com	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://fcmpushnotifications-1566b.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/193394991509/namespaces/firebase:fetch?key=AIzaSyCs7U_D56A5_I9DMCm2DSTC5vq46ixPp4 ）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 ProfileInstaller	Google	让库能够提前预填充要由 ART 读取的编译轨迹。
Jetpack AppCompat	Google	Allows access to new APIs on older API versions of the platform (many using Material Design).

敏感凭证泄露检测

可能的密钥

本报告由南明离火移动安全分析平台生成

"firebase_database_url" : "https://fcmpushnotifications-1566b.firebaseio.com"
"google_api_key" : "AIzaSyCs7U_D56Ao_LI9DMCm2DSTC5vq46ixPp4"
"google_app_id" : "1:19339499150:android:b206ca6a4caf863b2e1bdf"
"google_crash_reporting_api_key" : "AIzaSyCs7U_D56Ao_LI9DMCm2DSTC5vq46ixPp4"

Google Play 应用市场信息

标题: OneID

评分: 4.25 **安装:** 1,000+ **价格:** 0 **Android版本支持:** **分类:** 效率 **Play Store URL:** de.wurm.android.oneid

开发者信息: Wurm GmbH & Co. KG, Wurm+GmbH+%26+Co.+KG, None, https://www.wurm.de, account@frigodata.de,

发布日期: None **隐私政策:** Privacy link

关于此应用:

进入Wurm应用程序的最快方法-来自Wurm的OneID将移动设备绑定到用户ID。 使用Wurm Systems的OneID，您可以快速安全地访问Wurm应用程序。不再需要常规的登录过程。 OneID简化了对您经常使用的Wurm应用程序（例如FRIGODATA ONLINE）的访问。因此，您不再需要使用用户名和密码来完成登录过程。 为此，您可以使用该应用将移动设备（例如智能手机）绑定到Wurm系统中的用户ID。当您开始使用一个或多个Wurm应用程序时，始终会设置此唯一的用户ID。每个应用程序的所有个人权利和角色都链接到该ID。使用OneID应用程序将设备绑定到用户ID时，您还将包括系统上已建立的所有用户权限。然后，您可以使用智能手机或平板电脑上的OneID屏幕上的相应按钮，更快地登录到特定的应用程序。要使用此应用，您必须将移动设备绑定到您的用户ID。免费下载。检查过程并不复杂，可以通过检查您的个人电子邮件地址或手机号码（通过SMS）来完成。您的输入将在几秒钟内检查完毕。然后，您可以使用该应用程序以最快的速度访问自己的Wurm应用程序。例如，在工作设备（PC，便携式计算机等）上，打开FRIGODATA ONLINE（FDO）主页作为目标应用程序；在此（选择OneID登录过程之后），您必须输入用户名，然后按Enter。您将立即被识别为OneID用户。现在您所要做的就是点击智能手机上的FDO图标，您将立即登录FRIGODATA ONLINE。 您在个人OneID屏幕上看到的图标取决于您的用户ID。无论使用多少图标，您只要轻按一下手指即可达到目标。 当然，连接是经过加密的，并且可以满足所有Wurm解决方案所具有的高安全性要求。 2.0版的新功能 •通过推送通知登录 •通过智能手表登录 •管理您的设备 •全面翻新的用户界面 •黑暗模式 •许多小改进，使应用程序更易于使用

免责声明及风险提示