南明离火
移动应用检测平台

ANDROID 静态分析报告

helloword • v1.0

分析日期: 2024-05-18 16:11:16

应用概览

文件名称:	m.apk
文件大小:	0.79MB
应用名称:	helloword
软件包名:	com.example.helloword
主活动:	.MainActivity
版本号:	1.0
最小SDK:	8
目标SDK:	21
加固信息:	未加壳
应用程序安全分数:	28/100 (重大风险)
杀软检测:	2 个杀毒软件报毒
MD5:	73c16a3b6506d87c1990f0d3a6b82f84
SHA1:	0b0a6ed3b112d1d2aebcdedd7b30947[illegible]ed8049
SHA256:	3663471de7741fcf7df5629500fc[illegible]79e03d5f5c72264e96654b837d384aee

分析结果严重性分布

高危	中危	信息	安全	关注
4	1	0	1	0

四大组件导出状态统计

Activity组件：1个，其中export的有： 0个
Service组件：0个，其中export的有： 0个
Receiver组件：0个，其中export的有： 0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=US, O=Android, CN=Android Debug
签名算法: rsassa_pkcs1v15
有效期自: 2014-10-10 03:20:36+00:00
有效期至: 2044-10-02 03:20:36+00:00
发行人: C=US, O=Android, CN=Android Debug
序列号: 0x7e952642
哈希算法: sha256
证书MD5: 15fb7906b5da7134c154983440013eb7
证书SHA1: 11550d114df8683562c1be1a3f984e84f56ab7ce
证书SHA256: 07f2886655a73166240e96e706ab3981a974cf0bc4bcb8d643a6e3d91112660f
证书SHA512:
013306eae80a07d405297799ecea1e79dbd59267d024a47a3c066195abdeecf7ad0518475f0a317dd6461c04615a8cd8e0ffbb3f3a8a4dd8f017b5a474317fae

找到 1 个唯一证书

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: **2** | 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。
应用程序使用了调试证书进行签名	高危	应用程序使用了调试证书进行签名。生产环境的应用程序不能使用调试证书发布。

Manifest 配置安全分析

高危: **1** | 警告: **1** | 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 2.2-2.2.3, [minSdk=8]	警告	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	程序可被任意调试 [android:debuggable=true]	高危	应用可调试标签被开启，这使得逆向工程师更容易将调试器挂接到应用程序上。这允许导出堆栈跟踪和访问调试助手类。
3	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。

代码安全漏洞检测

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

序号	问题	等级	参考标准	文件位置

1	启用了调试配置。生产版本不能是可调试的	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

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	0/30	
其它常用权限	0/46	

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。

第三方 SDK 组件分析

SDK名称	开发者	描述信息
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。

敏感凭证泄露检测

可能的密钥
7631a988259a00816deda84afb29430a

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患。