南明离火
移动应用检测平台

ANDROID 静态分析报告

surat_girl • v1.0

分析日期: 2024-12-01 14:10:40

应用概览

文件名称:	surat_girl_558787894.apk
文件大小:	2.52MB
应用名称:	surat_girl
软件包名:	com.example.gnkqrzkkzs
主活动:	com.example.myapplication.SplashScreen
版本号:	1.0
最小SDK:	21
目标SDK:	30
加固信息:	未加壳
应用程序安全分数:	62/100 (低风险)
杀软检测:	13 个杀毒软件报毒
MD5:	019fec1b96838d519cdfbd4aea980cef
SHA1:	d0207ef5f9be700327e59990e7af4973e[illegible]e624
SHA256:	5d9c83d1a4e6fa195f34ccb036c[illegible]0b63[illegible]289012b272d910[illegible]de0b5c56f9fe

分析结果严重性分布

高危	中危	信息	安全	关注
0	9	1	2	0

四大组件导出状态统计

Activity组件：1个，其中export的有： 2个
Service组件：1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: True
v3 签名: False
v4 签名: False

主题: C=IN
签名算法: rsassa_pkcs1v15
有效期自: 2023-06-14 09:55:01+00:00
有效期至: 2048-06-07 09:55:01+00:00
发行人: C=IN
序列号: 0x1
哈希算法: sha256
证书MD5: cd27f110915cb0248f8f764d275c7b82
证书SHA1: e2fb3fdca83ffa9b1fc2101cddc91577a0b174a2
证书SHA256: 99063fedfac345d64b76f55a252f80fa55085f29726b9884edbc53c435b13c6b
证书SHA512:
e9b4f5da1b206abcf15202dd09c84c8676004f803e4a17ace4a9d29ee7fbd15db3b855a2dc1f9520b3d71a46b3ed38410b84e737d1de8b2a9bbd0b4ec0da0b34

公钥算法: rsa
密钥长度: 2048
指纹: 68aaeaa29e7ae76801ebd9ff336d9176faf9c6d634f6285fe781134097a7f8a8
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.RECEIVE_SMS	危险	接收短信	允许应用程序接收短信。 恶意程序会在用户未知的情况下监视或删除。
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

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.example.myapplication.SplashScreen	Schemes: sms://, smsto://, mms://, mmsto://, Mime Types: */*

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: **1** | 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

Manifest 配置安全分析

高危: **0** | 警告: **9** | 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 5.0-5.0.2, [minSdk=21]	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	应用程序已启用明文网络流量 [android:usesCleartextTraffic=true]	警告	应用程序打算使用明文网络流量，例如明文HTTP，FTP协议，DownloadManager和MediaPlayer。针对API级别27或更低的应用程序，默认值为“true”。针对API级别28或更高的应用程序，默认值为“false”。避免使用明文流量的主要原因是缺乏机密性，真实性和防篡改保护；网络攻击者可以窃听传输的数据，并且可以在不被检测到的情况下修改它。
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。
4	Activity-Alias (com.example.myapplication.activities.SplashActivity.Orange) 未被保护。 [android:exported=true]	警告	发现 Activity-Alias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-Alias (com.example.myapplication.activities.SplashActivity.BlackTheme) 未被保护。 [android:exported=true]	警告	发现 Activity-Alias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。
6	Broadcast Receiver (com.example.myapplication.MyReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.BROADCAST_SMS [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。
7	Service (com.example.myapplication.HeadlessSmsSendService) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.SEND_RESPOND_VIA_MESSAGE [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。
8	Broadcast Receiver (com.example.myapplication.PushReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.BROADCAST_WAP_PUSH [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。
9	Broadcast Receiver (com.example.myapplication.MmsSentReceiver) 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。
10	Broadcast Receiver (com.example.myapplication.MmsReceiver) 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。

代码安全漏洞检测

高危: **0** | 警告: **0** | 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

应用行为分析

编号	行为	标签	文件
00114	创建到代理地址的安全套接字连接	网络 命令	升级会员：解锁高级权限
00162	创建 InetSocketAddress 对象并连接到它	socket	升级会员：解锁高级权限
00163	创建新的 Socket 并连接到它	socket	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
00075	获取设备的位置	信息收集 位置	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

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	1/30	android.permission.RECEIVE_SMS
其它常用权限	1/46	android.permission.INTERNET

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。

敏感凭证泄露检测

可能的密钥
"key" : "23767ce256f7159

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