南明离火
移动应用检测平台

ANDROID 静态分析报告

Calculator • v12.2.00.4

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

分析日期: 2025-07-05 13:48:31

应用概览

文件名称:	86fbea1eabac4b19bdf091c128988d6984687688530a978fe79a5f9f9a477586.apk
文件大小:	3.97MB
应用名称:	Calculator
软件包名:	com.sec.android.app.popupcalculator
主活动:	com.sec.android.app.popupcalculator.Calculator
版本号:	12.2.00.4
最小SDK:	31
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:	73/100 (低风险)
杀软检测:	经检测，该文件安全
MD5:	8fa66fb92978b9adf50acc7954b4eb58
SHA1:	a33a15137527bff2b9f19c7e0b03d18c509dccbe
SHA256:	86fbea1eabac4b19bdf091c128988d6984687688530a978fe79a5f9f9a477586

分析结果严重性分布

高危	中危	信息	安全	关注
0	4	2	2	0

四大组件导出状态统计

Activity组件：5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

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

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=KR, ST=South Korea, L=Suwon City, O=Samsung Corporation, OU=DMC, CN=Samsung Cert, E=android.os@samsung.com
签名算法: rsassa_pkcs1v15
有效期自: 2011-06-22 12:25:13+00:00
有效期至: 2038-11-07 12:25:13+00:00
发行人: C=KR, ST=South Korea, L=Suwon City, O=Samsung Corporation, OU=DMC, CN=Samsung Cert, E=android.os@samsung.com
序列号: 0xe5eff0a8f66d92b3
哈希算法: sha1
证书MD5: 1ed6907e477e89c847cd7f7a971e0f46
证书SHA1: 9741a0f330dc2e8619b76a2597f308c37dbe30a2
证书SHA256: b9a42dd5fc4e054889ae4127a6274cec64e75c41733d42f5991e7019f9ea5caf
证书SHA512:
d2277c7f8731d24e7ba9f895e0b7b43086f17102f648fcfca20947149d6e7e9d01f15f657503e2b47208a648cab18445969fc75c7a6032a6639bd3d196522c04

公钥算法: rsa
密钥长度: 2048
指纹: 5e445885d51b5ca1824b02cd1da7e64cfbec95943b1ff2ab6e4d1cd56d73bed9
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
com.samsung.keyguard.SHORTCUT_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
com.sec.android.app.parser.permission.SecretCodeIME	未知	未知权限	来自 android 引用的未知权限。
android.permission.GET_TASKS	危险	检索当前运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。恶意应用程序可借此发现有关其他应用程序的保密信息。
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。
com.samsung.android.providers.context.permission.WRITE_USE_APP_FEATURE_SURVEY	未知	未知权限	来自 android 引用的未知权限。
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.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。
com.sec.spp.permission.TOKEN_b8a82002e8796582a00da99945c0030cbf5b2363606544cbe5839d0ed225f6ab6313360438d05c8f062aef9f4f0b12c876a16353cf9bd4732dcfb834d2addffa5f34e4b04344a60fa268dd722f793777fab4263f8be781f454a49e1c9362261e00cbd5b159b774555826c585f7f04e66134faca83b6f9e98441dcb54022e7d3e	未知	未知权限	来自 android 引用的未知权限。

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

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: **1** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用已启用明文网络流量 [android:usesCleartextTraffic=true]	警告	应用允许明文网络流量（如 HTTP、FTP 协议、DownloadManager、MediaPlayer 等）。API 级别 27 及以下默认启用，28 及以上默认禁用。明文流量缺乏机密性、完整性和真实性保护，攻击者可窃听或篡改传输数据。建议关闭明文流量，仅使用加密协议。

代码安全漏洞检测

高危: **0** | 警告: **3** | 信息: **2** | 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	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
3	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
4	应用程序使用SQLite数据库并执行原始SQL查询。原始SQL查询中不受信任的用户输入可能会导致SQL注入。敏感信息也应加密并写入数据库	警告	CWE: CWE-89: SQL命令中使用的特殊元素转义处理不恰当（'SQL 注入'） OWASP Top 10: M7: Client Code Quality	升级会员：解锁高级权限

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

5	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
6	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

应用行为分析

编号	行为	标签	文件
00013	读取文件并将其放入流中	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
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
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
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
00159	使用辅助服务执行通过文本获取节点信息的操作	无障碍服务	升级会员：解锁高级权限
00173	获取 AccessibilityNodeInfo 屏幕中的边界并执行操作	无障碍服务	升级会员：解锁高级权限
00125	检查给定的文件路径是否存在	文件	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	2/30	android.permission.GET_TASKS android.permission.VIBRATE
其它常用权限	2/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE

常用: 已知恶意软件广泛滥用的权限。

本报告由南明离火移动安全分析平台生成

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
data.forex.hexun.com	安全	否	No Geolocation information available.
dc.di.atlas.samsung.com	安全	否	**IP**地址: 34.120.24.208 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
regi.di.atlas.samsung.com	安全	否	**IP**地址: 34.120.24.208 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
• http://data.forex.hexun.com/data/mi/breedexch.html	com/sec/android/app/popupcalculator/converter/mortgage/svc/sp/hexun/HtmlInformation.java
• https://regi.di.atlas.samsung.com • https://dc.di.atlas.samsung.com	z0/c.java

Google Play 应用市场信息

标题: Samsung Calculator

评分: 4.5311403 **安装:** 1,000,000,000+ **价格:** 0 **Android**版本支持: **分类:** 工具 **Play Store URL:** com.sec.android.app.popupcalculator

开发者信息: Samsung Electronics Co., Ltd., 5200379633052405703, None, None, noreply.sec@samsung.com,

发布日期: 2017年2月8日 **隐私政策:** Privacy link

关于此应用:

[主要特点] 执行四项基本操作和工程计算。 要启动工程计算器，请点击工程计算器图标。 要检查计算历史记录，请点击计算历史记录图标。要关闭计算历史记录面板，请点击下键盘图标。 您可以使用以前输入的公式。从计算历史记录中点击所需的公式。 [附加功能] 要转换单位，请点按单位计算器按钮。您可以轻松转换各种类型的单位，例如面积，长度和温度。 该软件使用Apache License 2.0。有关详细信息，请访问 http://www.apache.org/licenses/LICENSE-2.0。

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

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。

© 2025 南明离火 - 移动安全分析平台自动生成

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成