南明离火
移动应用检测平台

ANDROID 静态分析报告

Packet Capture • v1.4.7

分析日期: 2024-05-11 13:48:06

应用概览

文件名称:	bas2e.apk
文件大小:	4.53MB
应用名称:	Packet Capture
软件包名:	app.greyshirts.sslcapture
主活动:	ui.HomeActivity
版本号:	1.4.7
最小SDK:	14
目标SDK:	26
加固信息:	未加壳
应用程序安全分数:	46/100 (中风险)
跟踪器检测:	3/432
杀软检测:	经检测，该文件安全
MD5:	edce2fbbf748df1d1d0ca3d6f00c9bc3
SHA1:	9646192eda047f589a0b68a841a713db783eae27
SHA256:	52f17c4979646f84ac5dd49cd39dfeacb9fe7061f061d28412c30066dc6a680c

分析结果严重性分布

高危	中危	信息	安全	关注
1	12	2	0	3

四大组件导出状态统计

Activity组件：13个，其中export的有： 0个
Service组件：3个，其中export的有： 2个
Receiver组件：4个，其中export的有： 2个
Provider组件：3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=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
签名算法: rsassa_pkcs1v15
有效期自: 2013-02-14 01:03:07+00:00
有效期至: 2040-07-02 01:03:07+00:00
发行人: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
序列号: 0x511c37cb
哈希算法: sha1
证书MD5: f7223136d549c5c715c979d312a0fac4
证书SHA1: 889ee6c8ec3c7dc460a5cec01620fa8b4a3f445e
证书SHA256: 6bc40417bcf746433ef778ed4e70437d498499a9e00b706fbbadc7c9aab06b57
证书SHA512:
58d5ba1142dfe0542b18bf49bbed64df8a212d4e4c1fe5ec26b720cbfbf02bf5f8566069d754df52257c80792a341deaa3492358870...824a6534671ef40af458

公钥算法: rsa
密钥长度: 2048
指纹: 38e7c6f6757674552091e9aea4b85f71b4f7048501a163d74ff4d7f48100af30
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.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。
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.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。
app.greyshirts.sslcapture.permission.C2D_MESSAGE	未知	未知权限	来自 android 引用的未知权限。

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: **5** | 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 4.0-4.0.2, [minSdk=14]	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。
3	Service (app.greyshirts.firewall.app.MyVpnService) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.BIND_VPN_SERVICE [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。
4	Broadcast Receiver (com.google.android.gms.measurement.AppMeasurementInstallReferrerReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.INSTALL_PACKAGES [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。
5	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: com.google.android.c2dm.permission.SEND [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。
6	Service (com.google.firebase.iid.FirebaseInstanceIdService) 未被保护。 [android:exported=true]	警告	发现 Service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: **1** | 警告: **5** | 信息: **2** | 安全: **0** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	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。敏感信息也应该加密并写入数据库	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
2	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

3	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
4	应用程序可以读取/写入外部存储器，任何应用程序都可以读取写入外部存储器的数据	警告	CWE: CWE-276: 默认权限不正确 OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	升级会员：解锁高级权限
5	该文件是World Writable。任何应用程序都可以写入文件	高危	CWE: CWE-276: 默认权限不正确 OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	升级会员：解锁高级权限
6	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
7	应用程序创建临时文件。敏感信息永远不应该被写进临时文件	警告	CWE: CWE-276: 默认权限不正确 OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	升级会员：解锁高级权限
8	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

Native 库安全加固检测

序号	动态库	NX(堆栈禁止执行)	PIE	STACK CANARY (栈保护)	RELRO	RPATH（指定SO搜索路径）	RUNPATH（指定SO搜索路径）	FORTIFY(常用函数加强检查)	SYMBOLS STRIPPED(裁剪符号表)

1	armeabi/libcore.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。		True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。 RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或 RPATH	None info 二进制文件没有设置 RUNPATH	False warning 二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数（如 strcpy，gets 等）的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用	False warning 符号可用

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.WAKE_LOCK
其它常用权限	4/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.WRITE_EXTERNAL_STORAGE 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
packet-capture.firebaseio.com	安全	否	**IP地址:** 35.201.97.85 **国家:** 美利坚合众国 **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
app-measurement.com	安全	是	**IP地址:** 180.163.151.166 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.224333 **经度:** 121.468948 **查看:** 高德地图

googleads.g.doubleclick.net	安全	是	**IP地址:** 180.163.151.166 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.224333 **经度:** 121.468948 **查看:** 高德地图
goo.gl	安全	否	**IP地址:** 172.217.175.14 **国家:** 美利坚合众国 **地区:** 加利福尼亚 **城市:** 山景城 **纬度:** 37.405991 **经度:** -122.078514 **查看:** Google 地图
www.bouncycastle.org	安全	否	**IP地址:** 103.32.[illegible].103 **国家:** 澳大利亚 **地区:** 维多利亚 **城市:** 墨尔本 **纬度:** -37.814007 **经度:** 144.963165 **查看:** Google 地图
fabric.io	安全	否	**IP地址:** 216.239.32.29 **国家:** 美利坚合众国 **地区:** 加利福尼亚 **城市:** 山景城 **纬度:** 37.405991 **经度:** -122.078514 **查看:** Google 地图
settings.crashlytics.com	安全	否	No Geolocation information available.
pagead2.googlesyndication.com	安全	是	**IP地址:** 180.163.151.166 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.224333 **经度:** 121.468948 **查看:** 高德地图
e.crashlytics.com	安全	否	No Geolocation information available.

URL 链接安全分析

URL信息	源码文件
• https://github.com/libuv/libuv • https://github.com/libuv/libuv/blob/master/LICENSE	自研引擎-A
• 10.0.8.1	app/greyshirts/firewall/app/MyVpnService.java
• 8.8.8.8	app/greyshirts/firewall/cache/DnsCache.java
• 2.5.4.32 • 2.5.4.72 • 2.5.29.36	

- 2.5.29.27
- 2.5.4.47
- 2.5.29.30
- 2.5.29.15
- 2.5.4.27
- 2.5.4.28
- 2.5.29.46
- 3.1.2.1
- 2.5.4.26
- 1.9.4.1
- https://www.google.com/dfp/inapppreview
- 2.5.4.25
- https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps
- https://www.google.com/dfp/linkdevice
- 2.5.4.12
- 2.5.4.42
- www.google.com
- http://www.google.com
- 2.5.4.49
- 2.5.29.33
- 2.5.29.20
- 2.5.29.16
- https://www.google.com/dfp/debugsignals
- 2.5.4.33
- https://app-measurement.com/a
- 2.5.4.41
- 2.5.4.19
- 2.5.4.10
- 8.8.8.8
- 2.5.4.3
- 2.5.4.65
- 2.5.4.17
- 2.5.29.17
- 2.5.29.9
- 2.5.4.43
- https://fabric.io/sign_up
- https://pagead2.googlesyndication.com/pagead/gen_204
- 2.5.29.55
- 2.5.29.29
- 2.5.29.23
- https://www.google.com/dfp/senddebugdata
- https://goo.gl/naoooi
- 2.5.4.24
- 1.3.1.1
- 2.5.29.35
- https://www.google.com
- 2.5.4.16
- 2.5.4.9
- 2.5.4.5
- 2.5.4.8
- 2.5.4.1
- 10.0.8.1
- 2.5.4.18
- 2.5.4.54
- 2.5.29.32
- 2.5.29.21
- 2.5.4.4
- 2.5.4.20
- 1.1.6.167
- 2.5.4.46
- 2.5.4.34
- 2.5.4.23
- 2.5.29.37
- 2.5.29.31

自研引擎-S

• 2.5.4.31 • https://e.crashlytics.com/spi/v2/events • 1.3.6.1 • 2.5.29.18 • 2.5.4.35 • https://settings.crashlytics.com/spi/v2/platforms/android/apps/%s/settings • 2.5.4.22 • 2.5.29.54 • 2.5.4.51 • https://packet-capture.firebaseio.com • 2.5.4.45 • 2.5.29.24 • 2.5.4.6 • 2.5.29.19 • 2.5.4.13 • 2.5.4.50 • 2.5.29.28 • http://www.bouncycastle.org • 2.5.4.44 • 2.5.29.56 • https://plus.google.com/ • 2.5.4.14 • 2.5.4.15 • 2.5.4.21 • 1.3.36.3 • 1.3.36.8 • 2.5.4.7 • 2.5.29.14	
• 10.20.30.42 • 10.20.30.44 • 10.20.30.41 • 10.20.30.46 • 10.20.30.45 • 10.20.30.47 • 10.20.30.40 • 10.20.30.43	lib/armeabi/libcore.so

Firebase 配置安全检测

标题	严重程度	描述信息

第三方 SDK 组件分析

SDK名称	开发者	描述信息
Crashlytics	Google	Crashlytics 是 Firebase 的主要崩溃报告工具。将众多崩溃整理成一个方便管理的问题列表，从而缩短问题排查时间。在 Crashlytics 信息中心内查看问题对用户造成的影响，从而清楚合理地确定应当首先解决哪些问题。
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。
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。

Firebase Analytics	Google	Google Analytics（分析）是一款免费的应用衡量解决方案，可提供关于应用使用情况和用户互动度的分析数据。

邮箱地址敏感信息提取

EMAIL	源码文件
test@test.test	app/ssldecryptor/CACertGenerator.java
test@test.test	自研引擎-S

第三方追踪器检测

名称	类别	网址
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

敏感凭证泄露检测

可能的密钥
凭证信息=> "io.fabric.ApiKey" : "9b1108c612ceae1c1c87298ef8e341c01bfc3cb"
"google_crash_reporting_api_key" : "AIzaSyAQEIN1WPt3pAxdxY93L5oK5XjzjNRq-eM"
"firebase_database_url" : "https://packet-capture.firebaseio.com"
"google_api_key" : "AIzaSyAQEIN1WPt3pAxdxY93L5oK5XjzjNRq-eM"
470fa2b4ae81cd56ecbcda9735803434cec591fa

Google Play 应用市场信息

标题: Packet Capture

评分: 2.9912024 **安装:** 1,000,000+ **价格:** 0 **Android版本支持:** **分类:** 工具 **Play Store URL:** app.greyshirts.sslcapture

开发者信息: Grey Shirts, Grey+Shirts, None, None, greyduchess@gmail.com,

发布日期: 2015年1月20日 **隐私政策:** Privacy link

关于此应用:

具有SSL解密的数据包捕获/网络流量嗅探器应用程序。 功能尚不丰富，但它是一个功能强大的调试工具，尤其是在开发应用程序时。 如果您无法捕获应用的SSL数据包 做以下其中一项：- 将targetSDKversion设置为23或更低 - 设置安全配置，描述为“针对Android 6.0（API级别23）和更低级别”的应用的默认配置 https://developer.android.com/training/articles/security-config.html#base-config 功能的 - 捕获网络数据包并记录它们。 - 使用中间人技术进行SSL解密。 - 不需要root，使用方便。 - 以十六进制或文本显示数据包。 您无需在PC上设置专用代理服务器。您只需要Android设备即可。 如何摆脱密码 如果您想在卸载数据包捕获后摆脱锁定屏幕上输入的PIN码，则需要清除凭据存储。 转到OS设置 - >安全性 - >清除凭据

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。