南明离火
移动应用检测平台

ANDROID 静态分析报告

HttpCanary • v3.3.6

分析日期: 2024-07-04 08:01:35

应用概览

文件名称:	HttpCanary_3.3.6.apk
文件大小:	6.1MB
应用名称:	HttpCanary
软件包名:	com.guoshi.httpcanary
主活动:	com.guoshi.httpcanary.ui.SplashActivity
版本号:	3.3.6
最小SDK:	28
目标SDK:	28
加固信息:	未加壳
应用程序安全分数:	58/100 (中风险)
杀软检测:	经检测，该文件安全
MD5:	70274da99f9a0d3cfa1a991374fc2e74
SHA1:	506e99a332faa8980295fab2c136f2fbbd8b33f2
SHA256:	b6ed57e07a5c46301782b9ee7e0f23323ef95af991a3e7f83924296997cfe653

分析结果严重性分布

高危	中危	信息	安全	关注
1	8	4	2	2

四大组件导出状态统计

Activity组件：10个，其中export的有：2个
Service组件：3个，其中export的有：1个
Receiver组件：0个，其中export的有：0个
Provider组件：2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: False
v2 签名: True
v3 签名: True

本报告由南明离火移动安全分析平台生成

v4 签名: False
主题: C=EN, ST=, L=, O=, OU=, CN=
签名算法: rsassa_pkcs1v15
有效期自: 2022-02-17 02:01:51+00:00
有效期至: 2066-02-06 02:01:51+00:00
发行人: C=EN, ST=, L=, O=, OU=, CN=
序列号: 0xea3a01
哈希算法: sha512
证书MD5: f70d178d608de64b28d4ae65a5f414e3
证书SHA1: 6f58c304e70d16be813f1bf80be04242fa65c9d4
证书SHA256: 76729bde7525da166e82860e66db4ce25195ac8ee8c554b8e4c9701fbad8cef1
证书SHA512:
caaec5b3ac1d5a518eb3a4d93db8c6a4e850dcfd39e80578631cdfc09c06ceaea0759016179c54636b18a2a83249c8af718aa4796f2df4433a[illegible]079de6b2e65

公钥算法: rsa
密钥长度: 8192
指纹: cd4af2f18514ef6479534f19b3a0309b514402853f2086c84e059cf55cdc2aed
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.READ_EXTERNAL_STORAGE	危险	读取SD卡内容	允许应用程序从SD卡读取信息。
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.REQUEST_INSTALL_PACKAGES	危险	允许安装应用程序	Android 8.0 以上系统允许安装未知来源应用程序权限。
android.permission.FOREGROUND_SERVICE	普通	创建前台Service	Android 9.0以上允许常规应用程序使用 Service.startForeground，用于podcast播放（推送悬浮播放，锁屏播放）
com.android.vending.CHECK_LICENSE	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。
android.permission.ACCESS_WIFI_STATE	普通	查看Wi-Fi状态	允许应用程序查看有关Wi-Fi状态的信息。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.guoshi.httpcanary.ui.content.FilePreviewResolverActivity	Schemes: file://, content://, http://, https://, Hosts: *, Mime Types: text/*, application/hcy, application/wscy, application/tcpcy, application/udpcy, application/octet-stream, Path Patterns: .*\\.hcy, .*\\.wscy, .*\\.tcpcy, .*\\.udpcy,
com.guoshi.httpcanary.ui.certificate.CertificateManagerActivity	Schemes: file://, content://, http://, https://, Hosts: *, Mime Types: application/x-pem-file, application/x-pkcs12, application/x-x509-user-cert, application/pkix-cert, application/x-x509-ca-cert, application/x-java-bc-keystore, application/x-x509-server-cert,

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	应用程序已使用代码签名证书进行签名

Manifest 配置安全分析

高危: **1** | 警告: **4** | 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存在漏洞的 Android 版本上 Android 9, minSdk=28]	信息	该应用程序可以安装在具有多个漏洞的旧版本 Android 上。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”。通过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	Activity (com.guoshi.httpcanary.ui.content.FilePreviewResolverActivity) is vulnerable to StrandHogg 2.0	高危	已发现活动存在 StrandHogg 2.0 劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (28) 更新到 29 或更高版本以在平台级别修复此问题。
4	Activity (com.guoshi.httpcanary.ui.content.FilePreviewResolverActivity) 未被保护。 [android:exported=true]	警告	发现 Activity 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 (com.guoshi.httpcanary.ui.certificate.CertificateManagerActivity) 未被保护。 存在一个intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。
6	Service (com.guoshi.httpcanary.AlwaysService) 受权限保护， 但是在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。

代码安全漏洞检测

高危: **0** | 警告: **4** | 信息: **4** | 安全: **1** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置

1	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
2	应用程序使用不安全的随机数生成器	警告	CWE: CWE-330: 使用不充分的随机数 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	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	此应用侦听剪贴板更改。一些恶意软件也会监听剪贴板更改	信息	OWASP MASVS: MSTG-PLATFORM-4	升级会员：解锁高级权限
5	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
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
7	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
8	此应用程序使用SQL Cipher。SQLCipher为sqlite数据库文件提供256位AES加密	信息	OWASP MASVS: MSTG-CRYPTO-1	升级会员：解锁高级权限
9	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

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	arm64-v8a/libbrotli.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

2	arm64-v8a/libglide-webp.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
3	arm64-v8a/libHttpCanary.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

4	arm64-v8a/libnetbare.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.REQUEST_INSTALL_PACKAGES
其它常用权限	6/46	android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.FOREGROUND_SERVICE android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE

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
httpcanary.com	安全	是	**IP地址:** 106.14.25.13 **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

docs.httpcanary.com	安全	是	**IP地址:** 106.14.25.13 **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

URL 链接安全分析

URL信息	源码文件
• https://httpcanary.com/web/zh/privacy.html • https://httpcanary.com/web/en/privacy.html	自研引擎-A
• https://docs.httpcanary.com/en/index.html • https://httpcanary.com/tutorials/en/index.html • https://httpcanary.com'	自研引擎-S

第三方 SDK 组件分析

SDK名称	开发者	描述信息
Brotli	Google	Brotli is a generic-purpose lossless compression algorithm that compresses data using a combination of a modern variant of the LZ77 algorithm, Huffman coding and 2nd order context modeling, with a compression ratio comparable to the best currently available general-purpose compression methods. It is similar in speed with deflate but offers more dense compression.
GlideWebpDecoder	zjupure	GlideWebpDecoder 是一个 Glide 集成库，用于在 Android 平台上解码和显示 webp 图像。它基于 libwebp 原生库并以 Fresco 和 GlideWebpSupport 的一些实现作为参考。
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。

邮箱地址敏感信息提取

EMAIL	源码文件
support@httpcanary.com	自研引擎-S

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。