南明离火
移动应用检测平台

ANDROID 静态分析报告

Gilli Danda • v1.1.5

分析日期: 2024-05-11 06:23:32

应用概览

文件名称:	com-ultpult-gilli-danda-16-56905762-bcf5cb835fbff288fa65b9651dd21e30.apk
文件大小:	46.06MB
应用名称:	Gilli Danda
软件包名:	com.ultpult.gilli.danda
主活动:	com.unity3d.player.UnityPlayerActivity
版本号:	1.1.5
最小SDK:	16
目标SDK:	26
加固信息:	未加壳
应用程序安全分数:	25/100 (重大风险)
跟踪器检测:	1/432
杀软检测:	3 个杀毒软件报毒
MD5:	bcf5cb835fbff288fa65b9651dd21e30
SHA1:	967eb145a976ac92632a4abb3[illegible]5e7dadb19c7ee
SHA256:	aee323f4184c7d57aabc[illegible]1a65eb5afddd22c5caec765774fa571457c899ea909

分析结果严重性分布

高危	中危	信息	安全	关注
4	4	1	0	3

四大组件导出状态统计

Activity组件：6个，其中export的有： 1个
Service组件：1个，其中export的有： 1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: CN=Ult Pult, OU=Game Studio, O=UltPult, L=Boston, ST=Massachusetts, C=+1
签名算法: rsassa_pkcs1v15
有效期自: 2016-06-24 18:30:19+00:00
有效期至: 2066-06-12 18:30:19+00:00
发行人: CN=Ult Pult, OU=Game Studio, O=UltPult, L=Boston, ST=Massachusetts, C=+1
序列号: 0x19fc75d9
哈希算法: sha1
证书MD5: c5cb79a888b06fc5c47896947a5ecc10
证书SHA1: c991e9cf94515573d6a9a57f176f822d11820b49
证书SHA256: 9ead545ebc1f55a7bf2fe6c2ee5f1a83c60bbb0d2b4faa4a8bc6915449c28328
证书SHA512:
a0a9a2ff5b09bcebfc2f4b93c0e0a633c54101ae9b501d29ce6d9c71bb3c182ac9ecf6615f5cacbcb7fe190e9ffcd2a940[illegible]22740600078cfc63cf948a32a

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。
com.android.vending.BILLING	普通	应用程序具有应用内购买	允许应用程序从 Google Play 进行应用内购买。
android.permission.ACCESS_NETWORK_STATE	普通	检索网络状态	允许应用程序查看所有网络的状态。
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。

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: **1** | 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。

Manifest 配置安全分析

高危: **2** | 警告: **3** | 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 4.1-4.1.2, [minSdk=16]	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	应用程序数据存在被泄露的风险 未设置[android:allowBackup]标志	警告	这个标志 [android:allowBackup]应该设置为false。默认情况下它被设置为true，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	Activity (com.unity3d.player.UnityPlayerActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
4	Activity （com.unity3d.player.UnityPlayerActivity） 容易受到 Android Task Hijacking/StrandHogg 的攻击。	高危	活动不应将启动模式属性设置为“singleTask”。 然后，其他应用程序可以将恶意活动放置在活动栈顶部，从而导致任务劫持/StrandHogg 1.0 漏洞。 这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”或设置空 taskAffinity (taskAffinity="") 属性来修复此漏洞。 您还可以将应用的目标 SDK 版本 (26) 更新到 28 或更高版本以在平台级别修复此问题。
5	Activity (com.unity.purchasing.googleplay.VRPurchaseActivity) 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.google.android.gms.auth.api.signin.RevocationBoundService) 受权限保护, 但是应该检查权限的保护级别。 Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [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。 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: **1** | 警告: **0** | 信息: **1** | 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	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

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-v7a/libmain.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	No RELRO high 此共享对象未启用 RELRO。整个 GOT（.got 和 .got.plt）都是可写的。如果没有此编译器标志，全局变量上的缓冲区溢出可能会覆盖 GOT 条目。使用选项 -z,relro,-z,now 启用完整 RELRO，仅使用 -z,relro 启用部分 RELRO	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.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。

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
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
www.paypal.com	安全	否	**IP地址:** 146.75.49.21 **国家:** 瑞典 **地区:** Vastra Gotalands lan **城市:** Goeteborg **纬度:** 57.707409 **经度:** 11.966732 **查看:** Google 地图
twitter.com	安全	否	**IP地址:** 104.244.42.129 **国家:** 美利坚合众国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.773968 **经度:** -122.410446 **查看:** Google 地图
www.linkedin.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
login.live.com	安全	否	**IP地址:** 20.190.144.161 **国家:** 大韩民国 **地区:** 首尔teukbyeolsi **城市:** 首尔 **纬度:** 37.566311 **经度:** 126.977203 **查看:** Google 地图
login.yahoo.com	安全	否	**IP地址:** 124.108.115.75 **国家:** 台湾省 **地区:** 台北 **城市:** 台北 **纬度:** 25.038172 **经度:** 121.563599 **查看:** Google 地图

pagead2.googlesyndication.com	安全	是	**IP地址:** 180.163.151.166 **国家:** 中国 **地区:** 上海 **城市:** None **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
• http://chilliant.blogspot.com.au/2012/08/srgb-aG • https://perf-events.cloud.unity3d.com/api/events/crashes • http://scripts.sil.org/OFL • http://www.styleseven.comFreeware • http://www.ascendercorp.com/ • https://docs.unity3d.com/Manual/UnityIAP.html • http://ultpult.com/mobappapi/upgame.php?apiname=GilliDanda • http://www.ultpult.com • http://www.ascendercorp.com/typedesigners.html • http://www.styleseven.comDigital • http://www.josbuivenga.demon.nl	自研引擎-A
• https://github.com/googlesamples/android-play-billing/issues/26	com/unity/purchasing/googleplay/IabHelper.java
• https://github.com/googlesamples/android-play-billing/issues/20 • https://www.google.com/dfp/senddebugdata • https://www.google.com/dfp/debugsignals • https://login.live.com • https://www.facebook.com • https://www.paypal.com • 127.0.0.1 • https://plus.google.com/ • https://www.google.com/dfp/inappprev... • www.google.com • https://accounts.google.com • https://pagead2.googlesyndication.com/pagead/gen_204 • https://login.yahoo.com • https://www.linkedin.com • https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps • https://www.google.com/dfp/linkdevice • http://www.google.com • https://twitter.com	自研引擎-S

第三方 SDK 组件分析

SDK名称	开发者	描述信息
Google Play Games plugin for Unity	Google	使游戏开发人员能在使用 Unity® 编写的游戏中集成 Google Play Games API。
Google Sign-In	Google	提供使用 Google 登录的 API。

本报告由南明离火移动安全分析平台生成

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。
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。

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

敏感凭证泄露检测

可能的密钥
凭证信息=> "com.google.android.gms.games.APP_ID" : "\ 587169014769"

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。