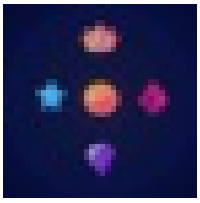
南明离火
移动应用检测平台

ANDROID 静态分析报告



Fortune Tiger • v0.0.2

分析日期: 2024-07-01 16:04:57

应用概览

文件名称:	Fortune Tiger_0.0.2_apkcombo.com.apk
文件大小:	32.14MB
应用名称:	Fortune Tiger
软件包名:	com.gem.enigma.threeinrow
主活动:	com.unity3d.player.UnityPlayerActivity
版本号:	0.0.2
最小SDK:	29
目标SDK:	33
加固信息:	未加壳
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:	a26a77717f199b3ccda1e2746fcb6f96
SHA1:	1dcb2e6a7ad4c4f9161b1e033e85bb0bfcfa340e
SHA256:	b4f4cf40a22972f2b87a3d1134[illegible]094c2f2e41fd4e4467fb21fd4919d6cfc

分析结果严重性分布

高危	中危	信息	安全	关注
0	2	1	1	0

四大组件导出状态统计

Activity组件：1个，其中export的有：0个
Service组件：0个，其中export的有：0个
Receiver组件：2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: True

v3 签名: True
v4 签名: False
主题: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
签名算法: rsassa_pkcs1v15
有效期自: 2024-06-03 11:32:39+00:00
有效期至: 2054-06-03 11:32:39+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0xbd3914ec18a7cafa1d68ac3db040cad815da6972
哈希算法: sha256
证书MD5: 00b48c9989326d17d6bae10cb380ba20
证书SHA1: 240c83d59019d0cdc5bb06d06c9534441c51b7a2
证书SHA256: f15db6e25a748432d0aeebb9347452fcc37b9e3dd5ed5c4911ab42b546bdaf21
证书SHA512:
bd3845bde4b61323925e2644b475a908c78fa0a604eac4c1feac307147794b862a18ff559d4118f20480cc64ed8d69540fb93bfe644581fe9476268949a51a27

公钥算法: rsa
密钥长度: 4096
指纹: 2b50d64a57756b014bb35218590bed9f354bde8c105ef1164e64f43f83a8de46
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。

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

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。

代码安全漏洞检测

高危: **0** | 警告: **1** | 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	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

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/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	Partial RELRO warning 此共享对象启用了部分 RELRO。 RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在部分 RELRO 中，GOT 部分的非 PLT 部分是只读的，但 .got.plt 仍然是可写的。使用选项 -z,relro,-z,now 启用完整的 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	0/30	
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。

URL 链接安全分析

URL信息	源码文件
• http://www.searchengineworld.com/validator/ • http://www.scoutjet.com/ • http://www.kosmix.com/html/crawler.html • http://browsers.garykeith.com • http://www.skycomp.ca • http://www.tecomi.com/bot.htm • http://www.google.com/bot.html • http://www.girafa.com • http://www.runnk.com/ • http://www.linktiger.com • http://www.opentagger.com/opentaggerbot.htm • http://www.herz-power.de/technik.html • http://www.sync2it.com/bms/susie.php • http://www.bloglines.com • http://www.coriolis.ch/ • http://www.whizbang.com/crawler • http://www.majestic12.co.uk/bot.php • http://buytaert.net/crawler/	

• http://subtextproject.com/ • http://www.dead-links.com/ • http://www.lipperhey.com/ • http://www.google.com/feedfetcher.html • http://www.scrubtheweb.com/abs/meta-check.html • http://www.europarchive.org • http://www.twingly.com/ • http://www.inktomi.com/slurp.html • http://www.domaincrawler.com/domains/view/ • http://www.busiverse.com/bot.php • http://minutillo.com/steve/feedonfeeds/ • http://tailrank.com/robot • http://www.SiteSpider.com/ • http://www.scifihifi.com/cocoalicious • http://www.dontbuylists.com/ • http://hilfe.acont.de/bot.html • http://chilliant.blogspot.com.au/2012/08/srgb-aG • http://www.google.com/adsbot.html • http://MapoftheInternet.com • http://www.catchbot.com • http://holmes.ge • http://www.jadynave.com/robot • http://www.activetourist.com • http://reader.livedoor.com/ • http://herbert.groot.jebbink.nl/?app=rssImages • http://www.kapere.com • http://corp.infocious.com/tech_crawler.php • http://www.yoow.eu • http://ponderer.org/ • http://search.thunderstone.com/texis/websearch/about.html • http://bookmarkbase.com • http://www.healthdash.com • http://www.kyluka.com/crawl.html • http://www.youdao.com/help/webmaster/spider/ • http://www.envolk.com/envolk • http://search.msn.com/msnbot.htm • http://gnomit.com/ • http://browsers.garykeith.com/sitemail/contact-me.asp • http://www.bestwhois.net/ • http://www.diffbot.com • http://www.ascendercorp.com/ • http://herbert.groot.jebbink.nl/?app=WebImages? • http://www.unwrap.jp • http://scripts.sil.org/OFL • http://Anonymouse.org/ • http://www.avantbrowser.com • http://www.goforit.com/about/? • http://net-promoter.com • http://www.tumblr.com/ • http://www.mojeek.com/bot.html • http://www.sqwidge.com/bot/ • http://scripts.sil.org/OFLhttp • http://www.ximian.com • http://www.live.com/ • http://wiki.creativecommons.org/Metadata_Scraper • http://botw.org • http://www.strategicboard.com • http://www.pagebull.com/ • http://www.inelue.com • http://misc.yahoo.com.cn/help.html • http://www.yama.info.waseda.ac.jp/ • http://www.cipinet.com/bot.html • http://www.meta-spinner.de/ • http://tinyurl.com/64t5n • http://www.html2jpg.com	自研引擎-A

- http://www.simpy.com/?ref=bot
- http://buytaert.net/crawler
- http://www.sync2it.com/susie
- http://www.feedhub.com
- http://otc.dyndns.org/webscan/
- http://www.answerbus.com/
- http://www.googlebot.com/bot.html
- http://knight.zook.in/
- http://www.displaydetails.com
- http://help.yahoo.com/help/us/ysearch/slurp
- http://www.kinja.com
- http://www.rojo.com/corporate/help/agg
- http://babelserver.org/rix
- http://www.entireweb.com
- http://www.inetbot.com/bot.html
- http://www.tipospereira.comhttp
- http://www.dotnetdotcom.org/
- http://www.ascendercorp.com/typedesigners.html
- http://www.newzcrawler.com/?
- http://www.briansmodelcars.com/links/
- https://github.com/marcelommp/Londrina-Typeface
- http://liferea.sf.net/
- http://doc.php.net

第三方 SDK 组件分析

SDK名称	开发者	描述信息
Unity	Unity Technologies	Unity 游戏使用 Il2Cpp 后端时产生的游戏代码。

Google Play 应用市场信息

标题: Fortune Tiger

评分: 3.4571428 **安装:** 10,000+ **价格:** 0 **Android版本支持:** **分类:** 益智 **Play Store URL:** com.gem.enigma.threeinrow

开发者信息: Foxconn it, Foxconn+it, None, None, olifarovaelika@gmail.com,

发布日期: 2024年6月6日 **隐私政策:** Privacy link

关于此应用:

欢迎来到 Fortune Tiger，这款终极三消益智游戏，让您玩上几个小时！潜入一个充满多彩宝石和具有挑战性关卡的世界，您的目标是连续匹配三个或更多相同的宝石以清除它们并得分。你消除的宝石越多，你的得分就越高！ 主要特点： 经典三消游戏老虎财富：易学易玩，但难以掌握。移动并对齐宝石以形成三个或更多的行。 定时挑战：通过基于时间的关卡测试您的快速思维和战略技能，并为 Tigrinho 得分目标。 众多关卡：享受无尽的乐趣，征服众多关卡，每个关卡都提供独特的挑战和目标。 物品计数器：使用特定的物品计数器跟踪您的进度，为游戏添加额外的策略层。 身临其境的氛围：体验充满活力的音乐和令人惊叹的音效的迷人游戏世界。 用户友好的界面：通过简单直观的界面轻松浏览游戏。 美丽的图形：享受视觉上吸引人的图形，使游戏体验更加愉快。 普遍吸引力：适合所有年龄段的玩家，无论您是益智爱好者还是只是在寻找一个有趣的方式来打发时间。 宝石之谜不仅仅是一个游戏；这是挑战思维和放松的绝佳方式。无论您的目标是获得高分，还是只是想享受充满活力的图形和引人入胜的声音，这款游戏适合每个人。 立即下载宝石之谜，在这款激动人心的三消冒险老虎游戏中测试您的智慧！

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。