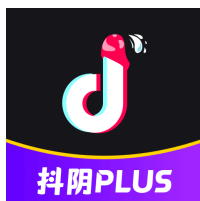




ANDROID 静态分析报告



抖阴Plus • v1.1.1

分析日期: 2024-07-28 14:52:32

i应用概览

文件名称:	dsII001_2024.7.14.000.apk
文件大小:	12.03MB
应用名称:	抖阴Plus
软件包名:	com.zq.dys
主活动:	com.zq.dys.MainActivity
版本号:	1.1.1
最小SDK:	22
目标SDK:	30
加固信息:	未加壳
应用程序安全分数:	51/100 (中风险)
杀软检测:	18 个杀毒软件报毒
MD5:	094dd09d28a45b64c3d07fc1c4d0520d
SHA1:	d1a0280236bf0c526fe0d231b5d2e3c25b067cef
SHA256:	398731e5380bb6bb8b3fc12a2f6c13cb1bffa93f62650c6d38c67c676ed344af92

📊分析结果严重性分布

🚨 高危	⚠️ 中危	ℹ️ 信息	✅ 安全	🔍 关注
1	2	1	1	0

📦四大组件导出状态统计

Activity组件: 1个, 其中export的有: 5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: 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: True

v2 签名: True
v3 签名: True
v4 签名: False
主题: C=a, ST=a, L=a, O=a, OU=a, CN=a
签名算法: rsassa_pkcs1v15
有效期自: 2022-06-21 05:32:57+00:00
有效期至: 2049-11-06 05:32:57+00:00
发行人: C=a, ST=a, L=a, O=a, OU=a, CN=a
序列号: 0x41772888
哈希算法: sha256
证书MD5: d49d20229d9dab896e21574bc3232c24
证书SHA1: 97b79fd8c8827cda42e464328c46dfb462f81b1e
证书SHA256: ba05c89d57a24934d976a647b91f733d38eb6f32d0c254b52aaba0ac1cc13b4b
证书SHA512:
4cf78e142e057f170c4bab11acec9f775015ff9539379b930d33d62c7587815ea44a53570eaa9b1ac1d1c4688d43d0d0a45c0a70cd86ddffcff7caaac0389fb

公钥算法: rsa
密钥长度: 2048
指纹: a8622d5e2214871f8de1d32546543dce06b23472ccf6ef958be849992a5043d9
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.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。
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	Android8.0 以上系统允许安装未知来源应用程序权限。
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。

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: 7
 | 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 5.1-5.1.1, [minSdk=22]	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”。避免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	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。
4	Activity-Alias (com.zq.dys.MainActivity5) 未被保护。 [android:exported=true]	警告	发现 Activity-Alias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-Alias (com.zq.dys.MainActivity4) 未被保护。 [android:exported=true]	警告	发现 Activity-Alias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。
6	Activity-Alias (com.zq.dys.MainActivity3) 未被保护。 [android:exported=true]	警告	发现 Activity-Alias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。
7	Activity-Alias (com.zq.dys.MainActivity2) 未被保护。 [android:exported=true]	警告	发现 Activity-Alias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。
8	Activity-Alias (com.zq.dys.MainActivity1) 未被保护。 [android:exported=true]	警告	发现 Activity-Alias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: 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	应用程序在加密算法中使用ECB模式 ECB模式是已知的弱模式，因为它对相同的明文块[UNK]产生相同的密文	高危	CWE: CWE-327: 使用已被攻破或存在风险的密码学算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-2	升级会员，解锁高级权限

2	SHA-1是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用已被攻破或存在风险的密码学算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	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

🚩 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)	SYMBOLSSTRIPPED(裁剪符号表)
----	-----	------------	-----	-------------------	-------	------------------	--------------------	-------------------	------------------------

1	arm64-v8a/libtoolChecker.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。	No ne info 二进制文件没有设置运行时搜索路径	No n o n e 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 libc 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	Fa ls e w a r n i n g 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	5/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE

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
-------	------

- https://player.vimeo.com/video/ - https://i.ytimg.com/vi/ - https://github.com/surmon-china - https://lf3-cdn-tos.bdxiguastatic.com/obj/ixigua-static/xigua_fe/xigua_video_web_pc/static/media/s - eries.bd5583e1.gif - https://html2canvas.hertzen.com - https://t.me/ - https://player.vimeo.com/api/player.js - https://clipboardjs.com/ - https://ldy.sc620.cc:19999/plusth001 - http://brianleroux.github.com/lawnchair/ - https://feross.org - https://www.youtube-nocookie.com - http://feross.org - https://noembed.com/embed?url=https - https://hertzen.com - https://xkeshi.github.io/image-compressor - https://pan.baidu.com/s/1wPIQE5srd_cGuPVqBWNUxw?pwd=1234 - https://douying.uk - https://cres.cuu771.com - https://vimeo.com/api/oembed.json?url= - https://feross.org/opensource - https://cdn.plyr.io/static/blank.mp4 - http://jsperf.com/b64tests - https://cdn.jsdelivr.net/npm/workbox-cdn - https://cdn.plyr.io/3.7.2/plyr.svg - https://raw.githubusercontent.com/stefanpenner/es6-promise/master/LICENSE - https://go.aniview.com/api/adserver6/vast/ - https://hfive.qsxon.com	自研引擎-A
---	--------

第三方 SDK 组件分析

SDK名称	开发者	描述信息
RootBeer	Scott Alexander-Brown	A tasty root checker library and sample app. We've scoured the internets for different methods of answering that age old question... Has this device got root?

敏感凭证泄露检测

可能的密钥
8f348975a3f4eedb6eee856f4b21d2fff77008f413be679bb2359b54acb9de17
8568bae0ad20b21cb7aa88e11d80b02120f51c6bfc67ca24dd01302912a6c36

3a3247ce8c09b07d2a30e0f3c32585d8
48c3e55a1f15413bb84b9c910d40f9db
deb8de36e04e554d4b778aee6814b94d
89ee2ba615248a4a88bdeb0b90f121e93d7297a259355c15eab9602ad8fe63e5
c2880140e5a58270bceb69326bb254ce
55183710c7c8f95892747db19936b526460929ee0934ea35f939b785e22e7039
8f59de91f7ca09e654eaa5889882bc73314057e4a0afc68296634ca0efeb78392ae9a95bce38ec72dba163d0b2872669
d0948cfb6da9174485e2b83949a6d36c
d95559629528fb410d0ed81c56dbd162
38ce953052956f25ada465bea5e3c3d1
7d0c180b61ff5a2fad476038f67b12f4
30add59a4c14c46001bcc1aa6b8729ea
tZh6iNz9LLDPawGUQGV6Y2ofUh6mraly
0e5c29f7e8b13ad7fa2493955096065c87e82f94a1e98b806b2953c1efcdd7cd
dd13168e82dc3b9154939f8c5fdb3188
1eb6e7de5eb956bb38a02245ed255ab3b08c2735707aca6014770712f3af1854
bab996deed2500571b76a06c77665c12
8c0f387b96a86b8e971332b61bff8602c2f1c4d6ffd2c4e3fa4560c3a9b70059
7f05b189662c5d7c18d12d2c1d98619d3f960fa0792a92692fec7c05d09f634
405187c2af01e0540e4ecb1268081c8e
d35129c0abe88ededfff9cf96e149b4cf37fa9e75300d56644b0ac4185b23aaf
b89d307765ac549771a67f6c69ef346c2ae9a95bce38ec72dba163d0b2872669
c495d7774ee5654f91b8dfb3d2123df2a82ad000513c0e33d88ac7d0d1668ed3
a0842fdd5e3045c7d91daec2ef2d341c65e25bec9d768725576701bf9df809b
1f053e35bff11d5678c49ba730029b0cae2e6d1f0d734951e99e8131afaa4513
ea131bff62ea3e5cf3c3f27f402a3c4
fff5af718c2b11e3a0c33a9ab9c80c5b
f9e78aa19b48e5859f64786f07f9dd3586dd17266ddd9ba74f96f48b55c54a69
af9c8eba903c9578aee774892ae1ac2b49a192f9111c0f071fce518f6f75ac7f
b5132dd0c8da8bbc90fd3c3f698b2830

c3c3b75661240c5797611c56db8f6629
0200a44a60a711d1ac877b5b64f1181fca9135b0468255d9f9a1fc0152d7edcd7619fd3c14ff5aaf6d12d0db9c823e7f
6acf67359eb3c02ee3406ed044f2c71d
d5302b1ef4bb7682b66f586e7d93414c
0c3ff7ee9d1612e3ed668b090bb21475
0b6c66808fbf5848f35870fc6e911f7920f51c6fbcf67ca24dd01302912a6c36
73111d7f055c71d37a4074acc336effb
9c2bfd0dd440375c00587ac62b6dbadd856c149252e522fce8d3502d39e66d2d84164b9d5eefb052eea58dcf9a6874cc
706b4d7bfd7aef7ebc1b4a9a70510f5b
930c13d64b94cf7cbfdbfa350c12708e
56c6278d99c12486685444f3cab1c8aafa0f92d26576dfdbdded998567de681b002d8170544613ee27a3e05de2883dfdc769ae2540dd32fe1ea23e292e83185a
1bb33f4b556767f6fc3a30244493376a04ff844b6289364d69d3742e91684e8d
36efccfae29adaeb5dedbe5db27266ef
95098d2ff465456beb502da84ebf44e92e1b7a3feaf6b256c751a1d43c13980f
37d63cabcb9877c3970f52e48b02cc4a3f960fa20752a92692fec7c05e00b634
2a7a15bd40d87df3d1a56c76c48fd6be5d8bc9f9fbe95b6d8b100f471a4fdd93
3fe9c3794be79b1bae5db562d22d83ab
ccc7ad03bad73c301873f264e947e7b3
781872d95ab65dd5f1ce287b4036e6b4
bb5d0f0f40b1d25088d094780cd0a6a5
7af1e1ff9387059e523016285e07c107
772d638044c16086a04cd90c765c13df04a0a6302ca601a8b4512a62b3fbee9
54db1fa657a176494b288780b26d710c20f51c6fbcf67ca24dd01302912a6c36
037bf1c4320cd2b3442dc3e4931f4948
cedc2918bfe81c8d0f168ed31cc9487
a27e2f9decce68acfeb20ae50ea0e5b7
d2eafd418ea80d4b768aad70b29c5d0ba42785cd169110077973d9d4d2991ff5
73c6100157a79a1b131e55db79cf269d
9c2bfd0dd440375c00587ac62b6dbadd5d954e456834a1bb837b1567629f104ae6cd3cfb855b6af0befa9f106795b0b0

6353f3b73e91b905b9f4a324a9d36e60
724e399de89be0fca0b30e7f1177a0af
6482466b953e915497c16389abf7d6f0
415c4ccda0bbaa14140d1dd267977f0b
4acfcd5743af9d86ac87c6ce519261e7
e009517243726c13b3130412a8c48587
a11649e5baa37cad461a43eb902dd4dd
36be43d0604c8e4528b9906979bf5144cefea4a35a48c1b21d5716211ec4c442
bfa347e277ee4d545ebd29dc248a062ee7b139545099f28595696c7565939b25
5ffca70840060b04516118c2f42f41188570f0da4293d9493f07b699843bdd043f960fa20752a92692fec7c05d09b634
91215a7eb7b7a98b3aac3b9d58018e3b98d02e2bbb3947fae9f6adb8ed006878
537b37d2e12d90d5dda3a27a0e4a68fc22f700a3f4d957b6963185e88a1e332e
aaada8a24fc4b65cb5de32c03cf9a625078d4a547daf9969d8bcdcd8165c5911
0620545af3d865929d62189069355b6b
08497481b9a1085dd3cf505d5a7053b80c5abff204a4dda25f12e049f85f043ef96d8db9cb14902aefc68cb584010a494a0031a85fbad888b1258cc4de0b01c
ed68020e80bf9370bdef28890af3cbf4
560880c9567c3f9c807f3e52c345692a13b5fe642097fccea7a4d898a2e9067
5ff8ce687f19965f4ef8bece534222ea
d229f932c48b254d61fcec6afe6081a63f960fa20752a92692fec7c05d09b634
db3ed36d746e3784cf54d3d0ee7f6ae892b13478c74cc5bf00196013cb23765c
991ee0585775d76b7ee9739ce20ecc9e4787d66e64a11adb50a11cf717492379e9a27753b6a6fb420ed7b927c1b698e81a47f10b49b2c926c3e110c6151122200da5ab8b18b8a42a79878d0f334a1dd7
73e69d810ad3f0a6ccc45bc4e6eacd57c2404a13e7db12aa3f56424f457ed88
d17bec62c635841c7e0e5ba52ffb552c
264a7c6135e0d89dba83c58a5a76a70b
0a4008a3f32ca7574f51b6e44a7ea2da
932f9fa330212c54d6622c36db52d20
fb239dc6770aa11a793918639992d761
329d18d618e0b8507df3a2820a4ad72e
a46f5af2657bfe882373c6bd6a96ff43

c242201f4276cd3a9af8bf3fd2959461
f2e5ee71b1ba98b08eaaec26b26e1e8c
4f4c5fd254c2f510e886463bba8df32e36781468d128525fa723f174349d81f1
f3859efa1a3978a0fba1eb5528e8b71d4283647840fda215cef8e0313504c5dd
8cbcf57a037852c6d9e90cb024491c50
54c3ccd78fe179e06bb5c0db4b0eff84
8aafc68945245c6fc33449529e281f18ff85b0ce668db92b443c0b8e378f36d1
1f01468e0fcd2eda63f37e362f7b0284
835e0d51538d2a0063cc922f96dc9e6f
f407d10bc584c07b9e1938bb242c9f45
8152b35787b79329f959f83ca52c9f8a572455f1266454df8a83d665a9b3c136
93ac17d31ae834dd59745616f160d4401ca13841333fc3a53ed0d43ef00b4ace
1b3c75a8123d0290a393a8991cfb3246
f3b4570804ed9e1415c0a44de1ab46773f960fa20752a92692fec7c05d09b634
2478b825a8a8198dc9e904670a47eb30efbae67440f9e45f12e19c39af9e4e2
df58ea9e07bb495eefae5dc4c946b21e

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。本报告内容仅供内部安全研究，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