南明离火
移动应用检测平台

ANDROID 静态分析报告

蓝月福利版 • v1.10.4

分析日期: 2025-04-14 19:19:50

应用概览

文件名称:	蓝月福利版 v1.10.4.apk
文件大小:	13.32MB
应用名称:	蓝月福利版
软件包名:	com.lyflbtomgnb1.h5.sp2
主活动:	com.tanwan.mobile.activity.TanwanH5InitActivity
版本号:	1.10.4
最小SDK:	20
目标SDK:	26
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	39/100 (高风险)
跟踪器检测:	1/432
杀软检测:	5 个杀毒软件报毒
MD5:	78f8baba479209f0dd92b1eb1aa79157
SHA1:	0f0c5889ab62b0fb52c8b582d47f232f77cb4fd2
SHA256:	4cba6d977e5a6e40e185f85c7fd644c8dfc709b4980ba37c32b98c9e8b5f12d

分析结果严重性

高危	警告	信息	安全	关注
7	18	2	1	23

四大组件信息

Activity组件：11个，其中export的有：3个
Service组件：5个，其中export的有：0个
Receiver组件：2个，其中export的有：2个
Provider组件：4个，其中export的有：0个

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=gz, ST=gz, L=gz, O=gz, OU=gz, CN=gz
签名算法: rsassa_pkcs1v15
有效期自: 2017-06-28 08:00:01+00:00
有效期至: 3016-10-29 08:00:01+00:00
发行人: C=gz, ST=gz, L=gz, O=gz, OU=gz, CN=gz
序列号: 0x691c8465
哈希算法: sha256
证书MD5: e3d010e5c2401f4d35c390ef154c437f
证书SHA1: 4f48d2e43bbf0346f05cea7e291240f81e88758a
证书SHA256: 0020e89c4aac5d589d8fd0353b1d188b9acfc06e87f80dd00c987a87cd4e63f5
证书SHA512:
ec41d83e06526d157300b097472132751be811b47588510dea9d9def06e363eb57f8115306c84e0ec5d41da62b5a776051d302180[illegible]b955c1234c61d6e1eb5b2

公钥算法: rsa
密钥长度: 2048
指纹: 870cab856bfbcb9ad2d7ac77ea89ea9a25d116a10814c1730ae4742c51f1d1cb
找到 1 个唯一证书

应用权限

权限名称	安全等级	权限内容	权限描述
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.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。
com.asus.msa.SupplementaryDID.ACCESS	普通	获取厂商oaid相关权限	获取设备标识信息oaid，在华硕设备上需要用到的权限。
freemme.permission.msa	未知	未知权限	来自 android 引用的未知权限。
android.permission.READ_PHONE_STATE	危险	读取手机状态和标识	允许应用程序访问设备的手机功能。有此权限的应用程序可确定此手机的号码和序列号，是否正在通话，以及对方的号码等。
android.permission.CHANGE_NETWORK_STATE	危险	改变网络连通性	允许应用程序改变网络连通性。
android.permission.CHANGE_WIFI_STATE	危险	改变Wi-Fi状态	允许应用程序改变Wi-Fi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。
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.READ_EXTERNAL_STORAGE	危险	读取SD卡内容	允许应用程序从SD卡读取信息。

可浏览的Activity组件

ACTIVITY	INTENT
com.tanwan.mobile.activity.TanwanH5InitActivity	Schemes: h5lczgsczb_949://,

com.tanwan.mobile.activity.TanwanH5GameActivity	Schemes: qn412c963f1d97://,

网络通信安全

序号	范围	严重级别	描述

证书安全分析

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	应用程序使用代码签名证书进行签名

MANIFEST分析

高危: **4** | 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。
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.tanwan.mobile.activity.TanwanH5GameActivity) 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。
4	Activity (com.alipay.sdk.app.PayResultActivity) 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。
5	Activity (com.alipay.sdk.app.PayResultActivity) 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。
6	Activity (com.alipay.sdk.app.AlipayResultActivity) 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。
7	Activity (com.alipay.sdk.app.AlipayResultActivity) 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。

8	Activity (com.alipay.sdk.app.AlipayResultActivity) 容易受到StrandHogg 2.0的攻击	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。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 (26) 更新到 29 或更高版本以在平台级别修复此问题。
9	Activity (com.alipay.sdk.app.AlipayResultActivity) 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。
10	Broadcast Receiver (com.tanwan.gamesdk.receiver.LogPrintBroadcastReceiver) 未被保护。 [android:exported=true]	警告	发现 Broadcast Receiver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。
11	Broadcast Receiver (com.tanwan.gamesdk.receiver.LogPrintBroadcastReceiver) 未被保护。 [android:exported=true]	警告	发现 Broadcast Receiver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。

</> 安全漏洞检测

高危: **3** | 警告: **9** | 信息: **2** | 安全: **1** | 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	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
3	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
4	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
5	MD5是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限

6	此应用程序可能具有Root检测功能	安全	OWASP MASVS: MSTG-RESILIENCE-1	升级会员：解锁高级权限
7	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
8	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
9	SHA-1是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
10	不安全的Web视图实现。可能存在WebView任意代码执行漏洞	警告	CWE: CWE-749: 暴露危险方法或函数 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限
11	可能存在跨域漏洞。在 WebView 中启用从 URL 访问文件可能会泄漏文件系统中的敏感信息	警告	CWE: CWE-200: 信息泄露 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限
12	如果一个应用程序使用WebView.loadDataWithBaseURL方法来加载一个网页到WebView，那么这个应用程序可能会遭受跨站脚本攻击	高危	CWE: CWE-79: 在Web页面生成时对输入的转义处理不恰当（'跨站脚本'） OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-6	升级会员：解锁高级权限
13	应用程序使用带PKCS5/PKCS7填充的加密模式CBC。此配置容易受到填充oracle攻击。	高危	CWE: CWE-649: 依赖于混淆或加密安全相关输入而不进行完整性检查 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	升级会员：解锁高级权限

14	使用弱加密算法	高危	CWE: CWE-327: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
15	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

动态库分析

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/libnative-lib.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。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程 (ROP) 攻击更难可靠地执行。	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	True info 符号被剥离
2	arm64-v8a/libsecurity.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。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程 (ROP) 攻击更难可靠地执行。	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	True info 二进制文件有以下加固函数: ['__vsprintf_chk', '__memmove_chk', '__memset_chk', '__memcpy_chk', '__strcpy_chk', '__vsnprintf_chk', '__strcat_chk', '__read_chk', '__strlen_chk']	True info 符号被剥离

3	arm64-v8a/libtattoo.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。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程 （ROP） 攻击更难可靠地执行。	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	True info 符号被剥离

行为分析

编号	行为	标签	文件
00022	从给定的文件绝对路径打开文件	文件	升级会员：解锁高级权限
00005	获取文件的绝对路径并将其放入 JSON 对象	文件	升级会员：解锁高级权限
00004	获取文件名并将其放入 JSON 对象	文件 信息收集	升级会员：解锁高级权限
00191	获取短信收件箱中的消息	短信	升级会员：解锁高级权限
00013	读取文件并将其放入流中	文件	升级会员：解锁高级权限
00062	查询WiFi信息和WiFi Mac地址	WiFi 信息收集	升级会员：解锁高级权限
00130	获取当前WiFi信息	WiFi 信息收集	升级会员：解锁高级权限
00033	查询IMEI号	信息收集	升级会员：解锁高级权限
00116	获取当前WiFi MAC地址并放入JSON中	WiFi 信息收集	升级会员：解锁高级权限
00076	获取当前WiFi信息并放入JSON中	信息收集 WiFi	升级会员：解锁高级权限
00082	获取当前WiFi MAC地址	信息收集 WiFi	升级会员：解锁高级权限
00063	隐式意图（查看网页、拨打电话等）	控制	升级会员：解锁高级权限
00012	读取数据并放入缓冲流	文件	升级会员：解锁高级权限

00051	通过setData隐式意图（查看网页、拨打电话等）	控制	升级会员：解锁高级权限
00096	连接到 URL 并设置请求方法	命令 网络	升级会员：解锁高级权限
00072	将 HTTP 输入流写入文件	命令 网络 文件	升级会员：解锁高级权限
00089	连接到 URL 并接收来自服务器的输入流	命令 网络	升级会员：解锁高级权限
00109	连接到 URL 并获取响应代码	网络 命令	升级会员：解锁高级权限
00094	连接到 URL 并从中读取数据	命令 网络	升级会员：解锁高级权限
00108	从给定的 URL 读取输入流	网络 命令	升级会员：解锁高级权限
00112	获取日历事件的日期	信息收集 日历	升级会员：解锁高级权限
00028	从assets目录中读取文件	文件	升级会员：解锁高级权限
00067	查询IMSI号码	信息收集	升级会员：解锁高级权限
00035	查询已安装的包列表	反射	升级会员：解锁高级权限
00054	从文件安装其他APK	反射	升级会员：解锁高级权限
00121	创建目录	文件 命令	升级会员：解锁高级权限
00119	将IMEI号写入文件	信息收集 文件 电话服务 命令	升级会员：解锁高级权限
00134	获取当前WiFi IP地址	WiFi 信息收集	升级会员：解锁高级权限
00125	检查给定的文件路径是否存在	文件	升级会员：解锁高级权限
00083	查询IMEI号	信息收集 电话服务	升级会员：解锁高级权限
00104	检查给定路径是否是目录	文件	升级会员：解锁高级权限
00192	获取短信收件箱中的消息	短信	升级会员：解锁高级权限
00036	从 res/raw 目录获取资源文件	反射	升级会员：解锁高级权限
00042	查询WiFi BSSID及扫描结果	信息收集 WiFi	升级会员：解锁高级权限
00153	通过 HTTP 发送二进制数据	http	升级会员：解锁高级权限
00030	通过给定的 URL 连接到远程服务器	网络	升级会员：解锁高级权限
00038	查询电话号码	信息收集	升级会员：解锁高级权限

00075	获取设备的位置	信息收集 位置	升级会员：解锁高级权限
00137	获取设备的最后已知位置	位置 信息收集	升级会员：解锁高级权限
00115	获取设备的最后已知位置	信息收集 位置	升级会员：解锁高级权限
00003	将压缩后的位图数据放入JSON对象中	相机	升级会员：解锁高级权限
00034	查询当前数据网络类型	信息收集 网络	升级会员：解锁高级权限

敏感权限分析

类型	匹配	权限
恶意软件常用权限	3/30	android.permission.REQUEST_INSTALL_PACKAGES android.permission.READ_PHONE_STATE android.permission.VIBRATE
其它常用权限	7/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.CHANGE_NETWORK_STATE android.permission.CHANGE_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。

域名检测

域名	状态	中国境内	位置信息
ip.twyx.cn	安全	是	**IP地址:** 106.15.92.55 **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
ipv6.twyx.cn	安全	否	No Geolocation information available.
sdklogapi.dunxiup.com	安全	是	**IP地址:** 122.228.195.237 **国家:** 中国 **地区:** 浙江 **城市:** 温州 **纬度:** 27.999420 **经度:** 120.666817 **查看:** 高德地图

gdtapi.tanwan.com	安全	是	**IP地址:** 220.185.164.223 **国家:** 中国 **地区:** 浙江 **城市:** 台州 **纬度:** 28.666668 **经度:** 121.349998 **查看:** 高德地图
ip.dunxiup.com	安全	是	**IP地址:** 106.15.92.55 **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
api.e.kuaishou.com	安全	是	**IP地址:** 58.215.85.106 **国家:** 中国 **地区:** 江苏 **城市:** 无锡 **纬度:** 31.569349 **经度:** 120.288788 **查看:** 高德地图
apisdk.tanwan.com	安全	是	**IP地址:** 182.40.124.114 **国家:** 中国 **地区:** 山东 **城市:** 青岛 **纬度:** 36.098610 **经度:** 120.371941 **查看:** 高德地图
sdklogapi.dunxiu123.com	安全	是	**IP地址:** 122.228.195.240 **国家:** 中国 **地区:** 江苏 **城市:** 镇江 **纬度:** 32.209366 **经度:** 119.434372 **查看:** 高德地图
ip.dunxiu123.com	安全	是	**IP地址:** 106.15.92.55 **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
gdtapi.dunxiu123.com	安全	是	**IP地址:** 122.228.195.236 **国家:** 中国 **地区:** 浙江 **城市:** 温州 **纬度:** 27.999420 **经度:** 120.666817 **查看:** 高德地图
sdkapi.dunxiup.com	安全	是	**IP地址:** 222.186.17.195 **国家:** 中国 **地区:** 江苏 **城市:** 镇江 **纬度:** 32.209366 **经度:** 119.434372 **查看:** 高德地图

sdkapi.tanwan.com	安全	是	**IP地址:** 106.15.92.55 **国家:** 中国 **地区:** 江苏 **城市:** 盐城 **纬度:** 33.385559 **经度:** 120.125282 **查看:** 高德地图
log.dunxiup.com	安全	是	**IP地址:** 122.225.209.231 **国家:** 中国 **地区:** 广东 **城市:** 深圳 **纬度:** 22.545673 **经度:** 114.068108 **查看:** 高德地图
m.tanwan.com	安全	是	**IP地址:** 122.228.195.240 **国家:** 中国 **地区:** 湖北 **城市:** 武汉 **纬度:** 30.583330 **经度:** 114.266853 **查看:** 高德地图
sdklogapi.tanwan.com	安全	是	**IP地址:** 61.160.227.233 **国家:** 中国 **地区:** 江苏 **城市:** 常州 **纬度:** 31.783331 **经度:** 119.966667 **查看:** 高德地图
www.tanwan.com	安全	是	**IP地址:** 61.160.227.234 **国家:** 中国 **地区:** 江苏 **城市:** 常州 **纬度:** 31.783331 **经度:** 119.966667 **查看:** 高德地图
ipv6.dunxiup.com	安全	否	No Geolocation information available.
sdkapi.dunxiu123.com	安全	是	**IP地址:** 220.185.164.225 **国家:** 中国 **地区:** 浙江 **城市:** 台州 **纬度:** 28.666668 **经度:** 121.349998 **查看:** 高德地图
pay.tanwan.com	安全	是	**IP地址:** 122.228.195.240 **国家:** 中国 **地区:** 浙江 **城市:** 温州 **纬度:** 27.999420 **经度:** 120.666817 **查看:** 高德地图

ad.partner.gifshow.com	安全	是	**IP地址:** 103.102.202.122 **国家:** 中国 **地区:** - **城市:** - **纬度:** 39.907501 **经度:** 116.397232 **查看:** 高德地图
log.dunxiu123.com	安全	是	**IP地址:** 222.186.17.199 **国家:** 中国 **地区:** 江苏 **城市:** 镇江 **纬度:** 32.209366 **经度:** 119.434372 **查看:** 高德地图
gdtapi.dunxiup.com	安全	是	**IP地址:** 222.186.17.203 **国家:** 中国 **地区:** 江苏 **城市:** 镇江 **纬度:** 32.209366 **经度:** 119.434372 **查看:** 高德地图
msdk.tanwan.com	安全	是	**IP地址:** 222.186.17.204 **国家:** 中国 **地区:** 江苏 **城市:** 镇江 **纬度:** 32.209366 **经度:** 119.434372 **查看:** 高德地图
ipv6.dunxiu123.com	安全	否	No Geolocation information available.
api.zeda1.com	安全	是	**IP地址:** 122.225.215.235 **国家:** 中国 **地区:** 广东 **城市:** 深圳 **纬度:** 22.545673 **经度:** 114.068108 **查看:** 高德地图
log.tanwan.com	安全	是	**IP地址:** 58.222.29.212 **国家:** 中国 **地区:** 江苏 **城市:** 台州 **纬度:** 32.492168 **经度:** 119.910767 **查看:** 高德地图
datahub.tanwan.com	安全	否	No Geolocation information available.

URL链接分析

URL信息	源码文件
• http://www.tanwan.com/api/hdlogin/sdk_android.php?phpsessid=	com/tanwan/gamesdk/activity/TwCommonWebActivity.java
• http://msdk.tanwan.com/androidlog.php • http://sdkapi.tanwan.com/v2022/popup_before • http://www.tanwan.com/app/xieyi.html • http://sdkapi.tanwan.com/v2022/fast_register	

• http://sdkapi.tanwan.com/v2022/user/account_up • http://sdkapi.tanwan.com/v2022/ly/sy_make_order • http://sdklogapi.tanwan.com/v2022/user_game_log • http://sdkapi.tanwan.com/v2022/get_login_phone_code • https://www.tanwan.com/api/mobile/sdk_passport.php • https://gdtapi.dunxiu123.com • https://apisdk.tanwan.com/passport.php • http://sdkapi.tanwan.com/v2022/init_before • http://sdklogapi.tanwan.com/v2022/install • http://sdkapi.tanwan.com/v2022/check_login_phone_code • https://sdklogapi.dunxiup.com • http://sdkapi.tanwan.com/v2022/login_confirm • http://sdkapi.tanwan.com/v2022/game_notice • http://sdkapi.tanwan.com/v2022/ly/sy_auth • https://gdtapi.tanwan.com/api/sdk_up_data.php • https://apisdk.tanwan.com/log/sdkerrorlog.php • https://log.tanwan.com • http://sdkapi.tanwan.com/v2022/cloud/init • http://sdkapi.tanwan.com/v2022/bind_phone • https://apisdk.tanwan.com/user/getuserinfo/ • http://sdkapi.tanwan.com/v2022/ly/pay_switch • http://sdkapi.tanwan.com/v2022/get_sms_code • http://sdkapi.tanwan.com/v2022/vip_desc • http://sdkapi.tanwan.com/v2022/pay/create • https://pay.tanwan.com/api/pay_query.php • https://pay.tanwan.com/api/sdk_v4/index.php • https://sdkapi.dunxiup.com • https://apisdk.tanwan.com/bindphoneswitch.php • http://sdkapi.tanwan.com/v2022/user_info • http://sdkapi.tanwan.com/v2022/check_phone • http://ip.dunxiu123.com • https://apisdk.tanwan.com • https://www.tanwan.com/api/backup_domain_v2.php • https://www.tanwan.com • http://sdkapi.tanwan.com/v2022/once_login • https://apisdk.tanwan.com/user/lytoken/ • http://sdkapi.tanwan.com/v2022/search_account • http://msdk.tanwan.com • http://sdkapi.tanwan.com/v2022/user/cancel_submit • http://ip.twyx.cn • http://sdkapi.tanwan.com/v2022/reset_password_code_check • https://sdkapi.dunxiu123.com • http://sdkapi.tanwan.com/v2022/pay_bind_phone • http://sdklogapi.tanwan.com • https://pay.tanwan.com/pay/getorderid/ • http://sdkapi.tanwan.com/v2022/check_sms_code • http://sdkapi.tanwan.com • http://ipv6.dunxiu123.com • https://gdtapi.tanwan.com/api/sy_toutiao_get_order.php • http://sdkapi.tanwan.com/v2022/pay/update_channel • http://sdkapi.tanwan.com/v2022/force_update • http://sdkapi.tanwan.com/v2022/ly/login_switch • http://sdkapi.tanwan.com/v2022/get_reset_password_code • http://sdkapi.tanwan.com/v2022/log_out • http://sdkapi.tanwan.com/v2022/register • https://apisdk.tanwan.com/state.php • https://sdklogapi.dunxiu123.com • https://apisdk.tanwan.com/user/gettoken/ • http://sdkapi.tanwan.com/v2022/reset_password • https://apisdk.tanwan.com/update.php • http://sdkapi.tanwan.com/v2022/order/get_user_record • https://log.tanwan.com/sdk/simulator • https://gdtapi.dunxiup.com • http://ip.dunxiup.com • http://sdklogapi.tanwan.com/v2022/event_trace • https://gdtapi.tanwan.com	com/tanwan/gamesdk/net/service/BaseService.java

• http://sdkapi.tanwan.com/v2022/order/get_order_state • https://log.tanwan.com/sdk/heart • https://apisdk.tanwan.com/p_change.php • http://sdkapi.tanwan.com/v2022/navigation_config • http://sdkapi.tanwan.com/v2022/popup_after • https://log.dunxiup.com • https://log.tanwan.com/sdk/event_trace • http://sdkapi.tanwan.com/v2022/init • http://sdkapi.tanwan.com/v2022/backup_domain • http://sdkapi.tanwan.com/v2022/vip_info • http://sdkapi.tanwan.com/v2022/user_fcm • http://ipv6.twyx.cn • http://sdkapi.tanwan.com/v2022/user/cancel_submit_v2 • https://log.dunxiu123.com • http://sdkapi.tanwan.com/v2022/scan_qr_login • http://sdkapi.tanwan.com/v2022/change_password • https://pay.tanwan.com • http://ipv6.dunxiup.com • http://sdkapi.tanwan.com/v2022/login • http://sdklogapi.tanwan.com/v2022/simulator	
• https://pay.tanwan.com/pay/getorderid/	com/tanwan/game/sdk/b/d_b.java
• http://www.tanwan.com/api/hdlogin/sdk_android.php?phpsessid=	com/tanwan/gamesdk/internal/usercenter/fragment/NewMessageFragment.java
• https://ad.partner.gifshow.com/api/v2/sdk/log?token=dee6172daef74f0895c7d1859[illegible]a7 • https://api.e.kuaishou.com/rest/config/client/v1/open/globalid	a/a/a/a/c.java
• http://datahub.tanwan.com/log.gif?activity=ods_sdk_heartbeat_log&uid=%s&user_name=%s&platform=%s • http://datahub.tanwan.com/log.gif?activity=ods_sdk_step_log&uid=%s&user_name=%s&platform=%s	com/tanwan/reportbus/util/UrlConfig.java
• http://www.tanwan.com/api/hdlogin/sdk_android.php?phpsessid= • https://m.tanwan.com/club/ • http://m.tanwan.com/wap/	com/tanwan/gamesdk/proguard/u_rr.java
• https://api.zeda1.com/api/bugly	com/zeda/crash/BaseService.java
• https://api.zeda1.com	com/hardy/boom/Constants.java
• 127.0.0.1	com/hardy/safeverify/device/IpScanner.java
• www.hashcode	com/tanwan/gamesdk/net/model/BackupDomainBean.java
• http://www.tanwan.com/api/hdlogin/sdk_android.php?phpsessid=	com/tanwan/gamesdk/internal/usercenter/tanwan/u_m.java
• 1.19.161.5	com/zeda/crash/net/Okhttp/OkHttpManger.java
• ws://article_9528?act=restore&from=tanwan	com/tanwan/gamesdk/c/a/c_a.java
• http://www.tanwan.com/api/hdlogin/sdk_android.php?phpsessid= • https://m.tanwan.com/club/ • http://m.tanwan.com/wap/	com/tanwan/gamesdk/dialog/TwUserCenterDialog.java
• http://m.tanwan.com/wap/	com/tanwan/gamesdk/fragmentdialog/TwExitDiglogFragment.java

本报告由南明离火移动安全分析平台生成

• https://msp.alipay.com/x.htm	com/tanwan/gamesdk/utils/Constants.java
• 1.19.161.5	com/zeda/crash/net/net/HttpUtility.java
• 127.0.0.1	uoo0oo0/uoo0oo0/uoo0oo0/uoo0oo0/uoo0oo0/uoo0oo0/OooO0O0.java

第三方SDK

SDK名称	开发者	描述信息
MSA SDK	移动安全联盟	移动智能终端补充设备标识体系统一调用 SDK 由中国信息通信研究院泰尔终端实验室、移动安全联盟整合提供，知识产权归中国信息通信研究院所有。
xCrash	iQIYI	xCrash 能为安卓 app 提供捕获 Java 崩溃，native 崩溃和 ANR 的能力。不需要 root 权限或任何系统权限。
支付宝 SDK	Alipay	支付宝开放平台基于支付宝海量用户，将强大的支付、营销、数据能力，通过接口等形式开放给第三方合作伙伴，帮助第三方合作伙伴创建更具竞争力的应用。
腾讯开放平台	Tencent	腾讯核心内部服务，二十年技术沉淀，助你成就更高梦想。
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

EMAIL	源码文件
tanwancom@126.com	com/tanwan/alipay/c_a.java

追踪器

名称	类别	网址
Tencent Stats	Analytics	https://reports.exodus-privacy.eu.org/trackers/116

密钥凭证

可能的密钥
凭证信息=> "TANWAN_APP_KEY" : "yWpx3hWQHFhSnTCj#11154#6KuRKuaAjLJ5sYRy"
凭证信息=> "ONE_LOGIN_APPID" : "c3fa6c3719fbe1f7cb22509b76932492"
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
87119ddb44a9ec4fc1e8a7c8d3303b7c
99P6evYumnhyp5uB73MtDii1328qGg1K
aVCxX2B3yswpxCMjaaSUHFXAzLYyuGhW

MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDIS8I37Y3yXAqVsRQmByfr8bcpBqq8NssxvL+EAOE5IPIQSYygeFX3y2hpIVTQETw6nzIynLX7aXjd+adKtrB874rQzLUEShk9t5qyLctN2QH/L83oMfi1q7Jj6QJKyuW2EKjjERdhCTq2agENBydU9Tdxa1UP2atAA43PlWdsowIDAQAB
dee6172daef74f0895c7d185956ac0a7
WV71xyttPKMoEzaOs5fxtr6JFBKMUFRU
6X8Y4XdM2Vhvn0KfzcEatGnWaNU=
wIA3XjJ67g6TS8yscMD0urZ6gyXUqLJi

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。