



ANDROID 静态分析报告



☛ 阳光分期 • v4.1.0

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

分析日期: 2024-08-01 10:50:34

i应用概览

文件名称:	阳光分期base.apk
文件大小:	15.96MB
应用名称:	阳光分期
软件包名:	hdghbdfc.ejibeeed.bcacaee
主活动:	com.yangguagnf.ui.activitys.JDXFOACT
版本号:	4.1.0
最小SDK:	22
目标SDK:	28
加固信息:	360加固 加固
应用程序安全分数:	28/100 (重大风险)
杀软检测:	AI评估: 可能有安全隐患
MD5:	134bdba3dcacc85687661426b3be82d7
SHA1:	0a32824393db26fd359ca7781a4fd9c9b73eeea8
SHA256:	e221b840c9a18ed22fe2e4d290951e235e12692951209ed3b917290fb3f95ab19

📊 分析结果严重性分布

🚨 高危	⚠️ 中危	i 信息	✓ 安全	🔍 关注
31	34	2	2	3

📦 四大组件导出状态统计

Activity组件: 42个, 其中export的有: 26个
Service组件: 1个, 其中export的有: 0个
Receiver组件: 2个, 其中export的有: 0个
Provider组件: 3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=Android, OU=Android, CN=Android, E=android@android.com

签名算法: rsassa_pkcs1v15

有效期自: 2008-02-29 01:33:46+00:00

有效期至: 2035-07-17 01:33:46+00:00

发行人: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com

序列号: 0x936eacbe07f201df

哈希算法: sha1

证书MD5: e89b158e4bcf988ebd09eb83f5378e87

证书SHA1: 61ed377e85d386a8dfee6b864bd85b0bfaa5af81

证书SHA256: a40da80a59d170caa950cf15c18c454d47a39b26989d8b640eccd745ba71bf5dc

证书SHA512:

5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccb6b34ec4233f5f640703581053abfea303977272d17958704d89b1711292a4569

公钥算法: rsa

密钥长度: 2048

指纹: f9f32662753449dc550fd88f1ed90e94b81adef9389ba16b89a6f3579c112e75

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_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.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.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.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.WRITE_CONTACTS	危险	写入联系人信息	允许应用程序修改您手机上存储的联系人（地址）数据。恶意应用程序可借此清除或修改您的联系人数据。
android.permission.READ_CONTACTS	危险	读取联系人信息	允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可借此将您的数据发送给其他人。
android.permission.READ_SMS	危险	读取短信	允许应用程序读取您的手机或SIM卡中存储的短信。恶意应用程序可借此读取您的机密信息。
android.permission.CAMERA	危险	拍照和录制视频	允许应用程序拍摄照片和视频，且允许应用程序收集相机在任何时候拍到的图像。
android.permission.WRITE_CALL_LOG	危险	写入通话记录	允许应用程序写入（但不读取）用户的通话记录数据。
android.permission.READ_CALL_LOG	危险	读取通话记录	允许应用程序读取用户的通话记录
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.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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
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.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_MEDIA_VISUAL_USER_SELECTED	危险	允许从外部存储读取用户选择的图像或视频文件	允许应用程序从用户通过权限提示照片选择器选择的外部存储中读取图像或视频文件。应用程序可以检查此权限以验证用户是否决定使用照片选择器，而不是授予对 READ_MEDIA_IMAGES 或 READ_MEDIA_VIDEO 的访问权限。它不会阻止应用程序手动访问标准照片选择器。应与 READ_MEDIA_IMAGES 和/或 READ_MEDIA_VIDEO 一起请求此权限，具体取决于所需的媒体类型。
android.permission.READ_MEDIA_IMAGES	危险	允许从外部存储读取图像文件	允许应用程序从外部存储读取图像文件。
android.permission.READ_MEDIA_VIDEO	危险	允许从外部存储读取视频文件	允许应用程序从外部存储读取视频文件。
android.permission.READ_MEDIA_AUDIO	危险	允许从外部存储读取音频文件	允许应用程序从外部存储读取音频文件。

🔒 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: 27 | 警告: 27 | 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.support.v4.app.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	Activity (com.yangguagnf.ui.activities.J0ACT) is vulnerable to StrandHogg 2.0	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 (28) 更新到 29 或更高版本以在平台级别修复此问题。
4	Activity (com.yangguagnf.ui.activities.J0ACT) is vulnerable to StrandHogg 2.0	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 (28) 更新到 29 或更高版本以在平台级别修复此问题。

5	Activity (com.yangguagnf.ui.activitys.J0ACT) 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.yangguagnf.ui.activitys.K0ACT) is vulnerable to StrandHogg 2.0	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 (28) 更新到 29 或更高版本以在平台级别修复此问题。
7	Activity (com.yangguagnf.ui.activitys.K0ACT) 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。
8	Activity (com.yangguagnf.ui.activitys.I0ACT) is vulnerable to StrandHogg 2.0	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 (28) 更新到 29 或更高版本以在平台级别修复此问题。
9	Activity (com.yangguagnf.ui.activitys.I0ACT) 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	Activity (com.yangguagnf.ui.activitys.MTH0ACT) is vulnerable to StrandHogg 2.0	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 (28) 更新到 29 或更高版本以在平台级别修复此问题。
11	Activity (com.yangguagnf.ui.activitys.MTH0ACT) 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。
12	Activity (com.yangguagnf.ui.activitys.MTG0ACT) is vulnerable to StrandHogg 2.0	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 (28) 更新到 29 或更高版本以在平台级别修复此问题。
13	Activity (com.yangguagnf.ui.activitys.MTG0ACT) 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。
14	Activity (com.yangguagnf.ui.activitys.L0ACT) is vulnerable to StrandHogg 2.0	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 (28) 更新到 29 或更高版本以在平台级别修复此问题。
15	Activity (com.yangguagnf.ui.activitys.L0ACT) 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。
16	Activity (com.yangguagnf.ui.activitys.MTM10ACT) is vulnerable to StrandHogg 2.0	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 (28) 更新到 29 或更高版本以在平台级别修复此问题。

17	Activity (com.yangguagnf.ui.activitys.MTM10ACT) 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。
18	Activity (com.yangguagnf.mjyp.BMAG01ACT) is vulnerable to StrandHogg 2.0	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 (28) 更新到 29 或更高版本以在平台级别修复此问题。
19	Activity (com.yangguagnf.mjyp.BMAG01ACT) 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。
20	Activity (com.yangguagnf.ui.activitys.N0ACT) is vulnerable to StrandHogg 2.0	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 (28) 更新到 29 或更高版本以在平台级别修复此问题。
21	Activity (com.yangguagnf.ui.activitys.N0ACT) 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。
22	Activity (com.yangguagnf.ui.activitys.M0ACT) is vulnerable to StrandHogg 2.0	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 (28) 更新到 29 或更高版本以在平台级别修复此问题。
23	Activity (com.yangguagnf.ui.activitys.M0ACT) 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。
24	Activity (com.yangguagnf.ui.activitys.MT6ACT) is vulnerable to StrandHogg 2.0	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 (28) 更新到 29 或更高版本以在平台级别修复此问题。
25	Activity (com.yangguagnf.ui.activitys.MT6ACT) 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。
26	Activity (com.yangguagnf.ui.activitys.Q0ACT) is vulnerable to StrandHogg 2.0	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 (28) 更新到 29 或更高版本以在平台级别修复此问题。
27	Activity (com.yangguagnf.ui.activitys.R0ACT) 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。
28	Activity (com.yangguagnf.ui.activitys.R0ACT) is vulnerable to StrandHogg 2.0	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 (28) 更新到 29 或更高版本以在平台级别修复此问题。

29	Activity (com.yangguagnf.ui.activities.R0ACT) 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。
30	Activity (com.yangguagnf.ui.activities.P0ACT) is vulnerable to StrandHogg 2.0	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 (28) 更新到 29 或更高版本以在平台级别修复此问题。
31	Activity (com.yangguagnf.ui.activities.P0ACT) 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。
32	Activity (com.yangguagnf.ui.activities.O0ACT) is vulnerable to StrandHogg 2.0	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 (28) 更新到 29 或更高版本以在平台级别修复此问题。
33	Activity (com.yangguagnf.ui.activities.O0ACT) 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。
34	Activity (com.yangguagnf.ui.activities.W0ACT) is vulnerable to StrandHogg 2.0	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 (28) 更新到 29 或更高版本以在平台级别修复此问题。
35	Activity (com.yangguagnf.ui.activities.W0ACT) 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。
36	Activity (com.yangguagnf.ui.activities.U0ACT) is vulnerable to StrandHogg 2.0	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 (28) 更新到 29 或更高版本以在平台级别修复此问题。
37	Activity (com.yangguagnf.ui.activities.U0ACT) 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。
38	Activity (com.yangguagnf.ui.activities.MT1ACT) is vulnerable to StrandHogg 2.0	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 (28) 更新到 29 或更高版本以在平台级别修复此问题。
39	Activity (com.yangguagnf.ui.activities.MT1ACT) 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。
40	Activity (com.yangguagnf.ui.activities.MTT3ACT) is vulnerable to StrandHogg 2.0	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 (28) 更新到 29 或更高版本以在平台级别修复此问题。

41	Activity (com.yangguagnf.ui.activities.MTT3ACT) 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。
42	Activity (com.yangguagnf.ui.activities.MT9ACT) is vulnerable to StrandHogg 2.0	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 (28) 更新到 29 或更高版本以在平台级别修复此问题。
43	Activity (com.yangguagnf.ui.activities.MT9ACT) 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。
44	Activity (com.yangguagnf.ui.activities.MT7ACT) is vulnerable to StrandHogg 2.0	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 (28) 更新到 29 或更高版本以在平台级别修复此问题。
45	Activity (com.yangguagnf.ui.activities.MT7ACT) 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。
46	Activity (com.yangguagnf.ui.activities.Z0ACT) is vulnerable to StrandHogg 2.0	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 (28) 更新到 29 或更高版本以在平台级别修复此问题。
47	Activity (com.yangguagnf.ui.activities.Z0ACT) 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。
48	Activity (com.yangguagnf.ui.activities.Y0ACT) is vulnerable to StrandHogg 2.0	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 (28) 更新到 29 或更高版本以在平台级别修复此问题。
49	Activity (com.yangguagnf.ui.activities.Y0ACT) 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。
50	Activity (com.yangguagnf.ui.activities.IdCardActivity) is vulnerable to StrandHogg 2.0	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 (28) 更新到 29 或更高版本以在平台级别修复此问题。
51	Activity (com.yangguagnf.ui.activities.IdCardActivity) 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。

52	Activity (com.yangguagnf.ui.activities.MTM0ACT) is vulnerable to StrandHogg 2.0	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 (28) 更新到 29 或更高版本以在平台级别修复此问题。
53	Activity (com.yangguagnf.ui.activities.MTM0ACT) 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。
54	Activity (com.wildma.pictureselector.PictureSelectActivity) is vulnerable to StrandHogg 2.0	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 (28) 更新到 29 或更高版本以在平台级别修复此问题。
55	Activity (com.wildma.pictureselector.PictureSelectActivity) 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。

</> 代码安全漏洞检测

高危: 4 | 警告: 6 | 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-332: 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-4	升级会员: 解锁高级权限
3	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
4	不安全的Web视图丢失。Web视图忽略SSL证书错误并接受任何SSL证书。此应用程序易受MITM攻击	高危	CWE: CWE-295: 证书验证不恰当 OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	升级会员: 解锁高级权限

5	已启用远程WebView调试	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
6	MD5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
7	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
8	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
9	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
10	不安全的WebView视图实现。可能存在WebView任意代码执行漏洞	警告	CWE: CWE-719: 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	该文件是World Writable。任何应用程序都可以写入文件	高危	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
12	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

13	<p>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</p>	高危	<p>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')</p> <p>OWASP Top 10: M1: Improper Platform Usage</p> <p>OWASP MASVS: MSTG-PLATFORM-6</p>	<p>升级会员: 解锁高级权限</p>
----	--	----	--	-------------------------------------

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)	SYMBOL STRIPPED (裁剪符号表)
1	arm4-v8a/libaliyunaf.so	<p>True</p> <p>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。</p>	True	<p>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。</p>	<p>Full RELRO</p> <p>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。</p>	None	<p>None</p> <p>info 二进制文件没有设置运行时搜索路径或 RPATH</p>	<p>False</p> <p>warning 符号可用</p>

2	arm64-v8a/libAPSE_7.0.1.so	<p>True info</p> <p>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。</p>	<p>True info</p> <p>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</p>	<p>Full RELRO info</p> <p>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。</p>	<p>No ne info</p> <p>二进制文件没有设置运行时搜索路径或 RPATH</p>	<p>No n e info</p> <p>二进制文件没有设置 RUNPATH</p>	<p>True info</p> <p>二进制文件有以下加固函数: ['_FD_ISSET_chk', '_FD_SET_chk']</p>	<p>False warning</p> <p>符号可用</p>
3	arm64-v8a/libAPSE_J.so	<p>True info</p> <p>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。</p>	<p>False high</p> <p>这个二进制文件没有在栈上添加栈哨兵值。栈哨兵是用于检测和防止攻击者覆盖返回地址的一种技术。使用选项 <code>-stack-protector-all</code> 来启用栈哨兵。这对于 Dart/Flutter 库不适用，除非使用了 Dart FFI</p>	<p>Full RELRO info</p> <p>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。</p>	<p>No ne info</p> <p>二进制文件没有设置运行时搜索路径或 RPATH</p>	<p>No n e info</p> <p>二进制文件没有设置 RUNPATH</p>	<p>False warning</p> <p>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 <code>strcpy</code>, <code>gets</code> 等) 的缓冲区溢出检查。使用编译选项 <code>-D_FORTIFY_SOURCE=2</code> 来加固函数。这个检查对于 Dart/Flutter 库不适用</p>	<p>False warning</p> <p>符号可用</p>

4	arm64-v8a/libfacedevice.so	<p>True info</p> <p>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。</p>		<p>True info</p> <p>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</p>	<p>Full RELRO info</p> <p>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。</p>	<p>No ne info</p> <p>二进制文件没有设置运行时搜索路径或 RPATH</p>	<p>No ne info</p> <p>二进制文件没有设置 RUNPATH</p>	<p>True info</p> <p>二进制文件有以下加固函数: ['_vsprintf_chk', '_memmove_chk', '_strchr_chk', '_memset_chk', '_memcpy_chk', '_strcpy_chk', '_vsnprintf_chk', '_strlen_chk']</p>	<p>False warning</p> <p>符号可用</p>
5	arm64-v8a/libtoyger.so	<p>True info</p> <p>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。</p>		<p>True info</p> <p>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</p>	<p>Full RELRO info</p> <p>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。</p>	<p>No ne info</p> <p>二进制文件没有设置运行时搜索路径或 RPATH</p>	<p>No ne info</p> <p>二进制文件没有设置 RUNPATH</p>	<p>False warning</p> <p>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</p>	<p>False warning</p> <p>符号可用</p>

6	arm64-v8a/libzkv_tj.so	<p>True info</p> <p>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。</p>	<p>False high</p> <p>这个二进制文件没有在栈上添加栈哨兵值。栈哨兵是用于检测和防止攻击者覆盖返回地址的一种技术。使用选项 <code>-fstack-protector-all</code> 来启用栈哨兵。这对于 Dart/Flutter 库不适用，除非使用了 Dart FFI</p>	<p>Full RELRO info</p> <p>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。</p>	<p>None info</p> <p>二进制文件没有设置运行时搜索路径或 RPATH</p>	<p>None info</p> <p>二进制文件没有设置 RUNPATH</p>	<p>False warning</p> <p>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 <code>strcpy</code>, <code>gets</code> 等) 的缓冲区溢出检查。使用编译选项 <code>-D_FORTIFY_SOURCE=2</code> 来加固函数。这个检查对于 Dart/Flutter 库不适用</p>	<p>False warning</p> <p>符号可用</p>
---	------------------------	--	--	---	--	--	--	---

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	9/30	android.permission.READ_PHONE_STATE android.permission.WRITE_CONTACTS android.permission.READ_CONTACTS android.permission.READ_SMS android.permission.SEND_SMS android.permission.WRITE_CALL_LOG android.permission.READ_CALL_LOG android.permission.RECORD_AUDIO android.permission.REQUEST_INSTALL_PACKAGES
其它常用权限	10/46	android.permission.INTERNET android.permission.ACCESS_WIFI_STATE android.permission.CHANGE_WIFI_STATE android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE android.permission.READ_EXTERNAL_STORAGE android.permission.CHANGE_NETWORK_STATE android.permission.READ_MEDIA_IMAGES android.permission.READ_MEDIA_VIDEO android.permission.READ_MEDIA_AUDIO

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

axzcvfeq-1324028813.cos.ap-guangzhou.myqcloud.com	安全	是	IP地址: 27.155.119.181 国家: 中国 地区: 福建 城市: 福州 纬度: 26.061390 经度: 119.306107 查看: 高德地图
nice800.com	安全	是	IP地址: 27.155.119.181 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
zxcvasdf-1326306285.cos.ap-guangzhou.myqcloud.com	安全	是	IP地址: 27.155.119.166 国家: 中国 地区: 福建 城市: 福州 纬度: 26.061390 经度: 119.306107 查看: 高德地图
www.beizhuabao.com	安全	否	No Geolocation information available.
kjalsdfnanzasdf.s3.ap-southeast-1.amazonaws.com	安全	否	IP地址: 52.219.184.30 国家: 新加坡 地区: 新加坡 城市: 新加坡 纬度: 1.289987 经度: 103.850281 查看: Google 地图

🌐 URL 链接安全分析

URL信息	源码文件
• http://www.beizhuabao.com	c/k/b/d/a/a.java
• http://www.beizhuabao.com	c/k/b/d/a/b.java
• https://nice800.com	com/yanguaguagnf/ui/activities/MT7ACT.java
• https://kjalsdfnanzasdf.s3.ap-southeast-1.amazonaws.com • https://axzcvfeq-1324028813.cos.ap-guangzhou.myqcloud.com • https://zxcvasdf-1326306285.cos.ap-guangzhou.myqcloud.com	c/k/b/d/a/e.java
• https://android-donwload.oss-cn-shanghai.aliyuncs.com/domain0dsfnname/5100sdfh0635.text/	c/k/b/d/a/d.java
• https://cn-shanghai-aliyun-cloudauth.oss-cn-shanghai.aliyuncs.com/model/toyger.face.dat • https://tianshu.alipay.com/504f3f0-aca8-4636-b486-e396559d3efb.png	c/f/a/n/k.java
• https://nice800.com	com/yanguaguagnf/ui/activities/MT10ACT.java
• https://renderer.alipay.com/p/yuyan/180020010001208736/aliyunfacewelcome.html	自研引擎-S

📦 第三方 SDK 组件分析

SDK名称	开发者	描述信息
金融级实名认证 SDK	Alibaba	金融级实名认证服务搭载真人检测和人脸比对等生物识别技术，配合权威数据源验证，可快速校验自然人的真实身份。
C++ 共享库	Android	在 Android 应用中运行原生代码。
360 加固	360	360 加固保是基于 360 核心加密技术，给安卓应用进行深度加密、加壳保护的安全技术产品，可保护应用远离恶意破解、反编译、二次打包，内存抓取等威胁。
AgentWeb	Justson	AgentWeb 是一个基于的 Android WebView，极度容易使用以及功能强大的库，提供了 Android WebView 一系列的问题解决方案，并且轻量和极度灵活。
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。

🔑 敏感凭证泄露检测

可能的密钥
凭证信息=> "com.amap.com.yangguagnf.mjyp.app.api.v2.apikey" : "0bsdfvdd0"
fd4ddd72c85fd5fe2913be520df32ed0
w7llxtix5zEhW1Qcm92aWRlck1hcGLHnMSFY8O6xls=
ZMO8xldix5zEheehruWummLHnMSFw7nHlsSH
x5pmxjNix5zEhWxpYmppYwd1X3g4Ni5zb2LHnMSFY2HEkw==
w7xkx1ix5zEhW1Mb2NhbFByb3ZpZGVyYsecxIXDumbEjQ==
x5RmxlvDvMeWxllzoZGdoYmRmYy5lamliZWVIZC5iy2EhW1Qcm92aWRlck1hcGLHnMSFY8O6xls=
ZGXEh2LHnMSFYW5kcm9pZC5hcHAuTG9hZGVkYXN5ZXI9Ym9keS5zEhW1Qcm92aWRlck1hcGLHnMSFY8O6xls=
YcO8xIvix5zEheaPkOekumLHnMSFZMecXNl=
MIGfMA0GCsGqSib3DQEBAQUAA4GNdCBiQKBgQC3DtFlK5C0hLgFu4IA3GAx4DAhLyag2Hsd2lsr1L66hH9SdefhaknsujWnumk+yNMYIQFdDnJ1Z8A4kj6zLJYRnNlyUeU0ti9uMlPr6AGUda78-BoK0YXJY6pxEw3w55oZmZjMswIRyv93o8fBKWx7mEnsrayE8VITzHroluQIDAQAB
Yseaxl3DvMeWxIk2MwVnMa3ZTg1ZDM4NmE4ZGZlZjYyYm9keS5zEhW1Qcm92aWRlck1hcGLHnMSFY8O6xls=
ZGPEkWLHnMSFYW5kcm9pZC5hcHAuTG9hZGVkYXN5ZXI9Ym9keS5zEhW1Qcm92aWRlck1hcGLHnMSFY8O6xls=
YseWxjNix5zEhW1Qcm92aWRlck1hcGLHnMSFY8O6xls=
7p+lxavEjW1LHnMSFLy5qaWFnd590ankuZmxhZ2LHnMSFw7run4jEjQ==
YsO6xldix5zEhS5qaWFnWCHnMSF7p+lxavEhw==
x5THlsSHYsecxIXb2Uc3RyYi5TdHViQXBwYsecxIXHlseUxlc=
x5RhxjPDvMeWxIk2MwVnMa3ZTg1ZDM4NmE4ZGZlZjYyYm9keS5zEhW1Qcm92aWRlck1hcGLHnMSFY8O6xls=
x5zHIMSTYsecxIUuamIhZ3Vix5zEhceUxavEkw==
ZseaxIvix5zEhW1QYWNrYwdISW5mb2LHnMSFw7rFq8SF

ab05c5fe1172477aa023e3046a6abbd2

w7rDvMSVYsecxIV4ODZfNjRix5zEhceWZMSB

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，深入扫描软件中潜在的漏洞和安全隐患。

© 2025 南明离火 - 移动安全分析平台自动生成

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成