南明离火
移动应用检测平台

ANDROID 静态分析报告

國海富 • v1.0.7

分析日期: 2025-10-05 08:57:39

应用概览

文件名称:	r8ssg.yal5k.dy3yw.fc8s5.apk
文件大小:	8.39MB
应用名称:	國 海 富
软件包名:	r8ssg.yal5k.dy3yw.fc8s5
主活动:	ubqanm.etwb7k.fbunu1.x5ltto.g5g3tc.kj93fj
版本号:	1.2.7
最小SDK:	24
目标SDK:	33
加固信息:	自定义加固
开发框架:	Java/Kotlin
应用程序安全分数:	50/100 (中风险)
跟踪器检测:	1/432
杀软检测:	AI评估：安全
MD5:	8da04e81b70c5bd09ca27500bf3f357b
SHA1:	efd99f32bce662c843e96b36be8eef907d7d82f6
SHA256:	889fe0733ca6340a293b0e5087733c097fbc3b24a8021330d893fa4ac2656e

分析结果严重性分布

高危	中危	信息	安全	关注
0	8	1	0	0

四大组件导出状态统计

Activity组件：7个，其中export的有： 2个
Service组件：0个，其中export的有： 0个
Receiver组件：0个，其中export的有： 0个
Provider组件：1个，其中export的有： 0个

应用签名证书信息

APK已签名
v1 签名: False
v2 签名: True
v3 签名: True
v4 签名: False
主题: C=adminhmr3xp, ST=adminhmr3xp, L=adminhmr3xp, O=adminhmr3xp, OU=adminhmr3xp, CN=adminhmr3xp
签名算法: rsassa_pkcs1v15
有效期自: 2025-09-03 15:47:02+00:00
有效期至: 2125-08-10 15:47:02+00:00
发行人: C=adminhmr3xp, ST=adminhmr3xp, L=adminhmr3xp, O=adminhmr3xp, OU=adminhmr3xp, CN=adminhmr3xp
序列号: 0x2d828060
哈希算法: sha256
证书MD5: 21aba023d493966b4803f21fa56f3919
证书SHA1: 997db14a7099865424c2f3bc8e86a6d702eb08ae
证书SHA256: 18837597af4fd2ed0c9daa5b25c927c5060806ce036a4c514057e984111e9631
证书SHA512:
d4b5891e9d89ed1f408b432e6c3ccfa556134d2b4076fbc775958cc779a34a39a29049da99ec6e5d1d4c49e229ba6ee6494b9da47cdafc91b3f6ec61808f974f

公钥算法: rsa
密钥长度: 1024
指纹: b04e5fcffdd639dd97628f142a2390bf57598740e251f4d50e21fd05edb25bbd
共检测到 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.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。

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: **0** | 信息: **1**

标题	严重程度	描述信息
已签名应用	信息	应用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: **3** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用已启用明文网络流量 [android:usesCleartextTraffic=true]	警告	应用允许明文网络流量（如 HTTP、FTP 协议、DownloadManager、MediaPlayer 等）。API 级别 27 及以下默认启用，28 及以上默认禁用。明文流量缺乏机密性、完整性和真实性保护，攻击者可窃听或篡改传输数据。建议关闭明文流量，仅使用加密协议。

2	应用已配置网络安全策略 [android:networkSecurityConfig=@7F130002]	信息	网络安全配置允许应用通过声明式配置文件自定义网络安全策略，无需修改代码。可针对特定域名或应用范围进行灵活配置。
3	Activity (ubqanm.etwb7k.fbunu1.x5ltto.g5g3tc.l9ty4w) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
4	Activity (ubqanm.etwb7k.fbunu1.x5ltto.g5g3tc.prh2ek) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。

代码安全漏洞检测

高危: **0** | 警告: **3** | 信息: **1** | 安全: **0** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	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
2	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
3	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
4	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

Native 库安全加固检测

本报告由南明离火移动安全分析平台生成

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/libnmmp.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缓冲区检测。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

应用行为分析

编号	行为	标签	文件
00013	读取文件并将其放入流中	文件	升级会员：解锁高级权限
00024	Base64解码后写入文件	反射 文件	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

本报告由南明离火移动安全分析平台生成

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
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
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
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

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.CAMERA
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。

恶意域名威胁检测

域名	状态	中国境内	位置信息
home.openweathermap.org	安全	否	**IP地址:** 167.99.222.135 **国家:** 荷兰（王国） **地区:** 北荷兰省 **城市:** 阿姆斯特丹 **纬度:** 52.378502 **经度:** 4.899980 **查看:** Google 地图
api.openweathermap.org	安全	否	**IP地址:** 167.99.222.135 **国家:** 德国 **地区:** 萨克森 **城市:** 法尔肯施泰因 **纬度:** 50.477852 **经度:** 12.371563 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• https://home.openweathermap.org/api_keys • https://api.openweathermap.org/data/2.5/	ubqanm/etwb7k/fbunu1/x5ltto/rzywny/z2685h.java

第三方 SDK 组件分析

SDK名称	开发者	描述信息

Bugly	Tencent	腾讯 Bugly，为移动开发者提供专业的异常上报和运营统计，帮助开发者快速发现并解决异常，同时掌握产品运营动态，及时跟进用户反馈。
MMKV	Tencent	MMKV 是基于 mmap 内存映射的 key-value 组件，底层序列化/反序列化使用 protobuf 实现，性能高，稳定性强。
nmmp	maoabc	nmmp 是一个用于保护 Android 类的 dex 文件的库，它使用 dex-vm 技术将类和方法转换为字节码，从而防止反编译。
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。
Jetpack App Startup	Google	App Startup 库提供了一种直接，高效的方法来在应用程序启动时初始化组件。库开发人员和应用程序开发人员都可以使用 App Startup 来简化启动顺序并显式设置初始化顺序。App Startup 允许您定义共享单个内容提供程序的组件初始化程序，而不必为需要初始化的每个组件定义单独的内容提供程序。这可以大大缩短应用启动时间。

第三方追踪器检测

名称	类别	网址
Bugly		https://reports.exodus-privacy.eu.org/trackers/190

敏感凭证泄露检测

可能的密钥
x5hhxIthw7nEj1Vua25vd24gdmlzaWJpbGl0eSBhw7nEj2RmxIs=
ZseWxIvHnGbEkyBmaWxlTmFtZTrHnGbEk2XHmsSL
ZmPEg8ecZsSTRGVsZWdhdGVBcHBsaWNhdGlvbi5vbkNyZWF0ZTA6x5xmxJNj7p+IxM=
ZceUxI/HnGbEk2N1cnJlbnRBY3RpdmI0eVhpcnVhZMecZsSTY8WrxI8=
7p+IYsSFx5xmxJNob29rM8ecZsSTx5ZiJUE=
YWHEg8ecZsSTPT09PT0+x5xmxJNuM4hJxIM=
x5bHmMSFYcO5xI8gdGZsYWJlTSUJMRWHDucSPYsWrxIM=
x5xmxJXHnGbEk2NlcGxhY2VDb250ZW50UHJvdmlkZXJxx5xmxJPHmO6fiMSB
x5ZmxJVhnZnEivB0byBJTlZJU0lCTEVhM7nEj2XFq8SB
x5zDucSFx5xmxJNyZXBsYWNlOl9uaGVudFByb3ZpZGVyM8ecZsSTx5bHmsSF
x5jHlMSJYcO5xI8gZnJvb3ib250YWluZXIgYcO5xI9jx5TEiQ==
Y8eYxI3HnGbEk2FtZHJvaWQuYXBwLkFjdGl2aXR5VGhyZWFkx5xmxJPHmMeYxI0=
7p+Ix5jEg2MDucSPYklTSUJMRWHDucSPx5bHmsSD
x5rHmsSHlcO5xI9TcGVjaWFsRWZmZWN0c0NvbnRyb2xsZXI6IFJlbW92aW5nIHZpZXcgYcO5xI9hw7zEhw==
YceWxIvHnGbEk21BcHBsaWNhdGlvbsecZsSTx5xlxIs=

x5TDvMSVx5xmxJNhbmRyb2lkLmNvbnRlbnQuQ29udGVudFByb3ZpZGVyx5xmxJPun4jHlsSB
x5THnMSFx5xmxJNzZXRPdXRlckNvbnRleHTHnGbEk2bDucSF
x5jFq8SLYcO5xI9SRU1PVklOR2HDucSPZGXEiw==
w7xmxIfDuseYxIdhbmRyb2lkLmNvbnRlbnQucG0uUGFja2FnZU1hbmFnZXLDuseYxIfFq2TEiQ==
x5RixJPHnGbEk0RlbGVnYXRlQXBwbGljYXRpb24ub25DcmVhdGUxx5xmxJPun4hjxJM=
x5THmMSRYcO5xI9GcmFnbWVudE1hbmFnZXJhw7nEj2PDusSR
w7rHmMSNx5xmxJMgfCBhLmPHnGbEk8O8xavEjQ==
x5Tun4jEh8ecZsSTbU1haW5UaHJlYWTHnGbEk2THlMSH
xatmxInHnGbEkz09PT09PsecZsSTZWTEiQ==
YcO8xJVhw7nEj0JPVFRPTWHDucSPw7pixIE=
x5jHlsSFx5xmxJNvbkNyZWF0ZUV4M8ecZsST7p+Iw7rEhQ==
YmLEk2HDucSPU3BlY2lhbEVmZmVjdHNDb250cm9sbGVyOiBTZXR0aW5nIHZpZXcgYcO5xI/un4hmxJM=
YsecxI3HnGbEk21QYWNrYWdlSW5mb8ecZsSTZMO6xI0=
xavHnMSTx5xmxJNtTG9jYWxQcm92aWRlcsecZsSTZceUxJM=
x5xhxJHHnGbEk29uQ3JlYXRlRXgyOsecZsSTYsecxJE=
x5pkxJNhw7nEj0lOVklTSUJMRWHDucSPYWPEkw==
7p+Iw7nEi8ecZsSTQUVTL0NCQy9QS0NTNVBhZGRpbmfHnGbEk+6fiMO8xls=
ZmPEj8ecZsSTbUFwcGxpY2F0aW9ux5xmxJNkYsSP
ZMecxJHHnGbEk21Qcm92aWRlck1hcMecZsSTZseexJE=
ZcecxInHnGbEk21Jbml0aWFsQXBwbGljYXRpb27HnGbEk+6fiMO5xIk=
YmHEh8ecZsSTb25DcmVhdGVEeDE6x5xmxJNlZMSH
w7zHlMSRx5xmxJNtQXBwbGljYXRpb25JbmZvx5xmxJHDusO6xIE=
YsO8xI9hw7nEj0NHTlRFUU9YcO5xI/DuseYxI8=
jp8xpyd6nja0rcx9fn1yqvx8tyx5vutrvkliq1wl3ezjsud
x5rHmMSNx5xmxJMgY29udGV4dDrHnGbEk8WrY8SN
YceYxIXHnGbEk3JlcGxhY2VDb250ZW50UHJvdmlkZXlyx5xmxJPDumPEhQ==
w7llxJXHnGbEkyUxIC0xNlPHnGbEk8eaZMSB
w7rDucSVx5xmxJNEZWVxlZ2F0ZUFwcGxpY2F0aW9uLm9uQ3JlYXRlMsecZsSTY2bEgQ==
w7nHmsSJx5xmxJNhbmRyb2lkLmFwcC5Mb2FkZWRBcGvHnGbEk8eWx5TEiQ==
ZcO6xIlhw7nEj251bGxhw7nEj8eUxavEiQ==

w7lmxI1hw7nEj0NFTlRFUl9ZYcO5xI/HmMeUxI0=
7p+I7p+IxIvDuseYxIdNQU5JRkVTVC5NRsO6x5jEh2NjxI0=
ZGLEicecZsSTb25DcmVhdGVFeDXHnGbEk8eaZsSJ
x5zFq8SJx5xmxJNnZXRJbnN0YW5jZcecZsSTw7pkxIk=
YseUxJNhw7nEj0JBU0VMSU5FYcO5xI/HmsO8xJM=
w7xmxJPHnGbEk2FuZHJvaWQuYXBwLkxvYWRlZEFwa8ecZsSTx5TDusST
7p+IZMSNYcO5xI9BRERJTkdhw7nEj2THnMSN
aHR0cHM6Ly9oZGZ1eXVrLTEzNzE0ODYwNTguY29zLmFjY2VsZXJhdGUubXlxY2xvdWQuY29tLw==
x5ZixIvHnGbEk21BbGxBcHBsaWNhdGlvbnPHnGbEk2XHmMSL
ZsWrxIfHnGbEk29uQ3JlYXRlRXg0x5xmxJPDvGHEhw==
ZMO8xIPHnGbEkz09PT09PnJlcGFwcMecZsSTY2XEgw==
w7lkxIPHnGbEk2F0dGFjaMecZsSTw7zHlMSD
ZceaxJXHnGbEk2FuZHJvaWQuYXBwLkFjdGl2aXR5VGhyZWFkx5xmxJPHlmHEgQ==
xavHmsSJw7rHmMSHZ2V0QXBwbGljYXRpb25JbmZvw7rHmMSHx5TDusSL
Zu6fiMSHx5xmxJNtUGFja2FnZUluZm/HnGbEk8Wrw7nEhw==
x5rHlMSNw7rHmMSHMTc1Njk0MzMxNzgxNcO6x5jEh8eYx5zEjw==
x5ZmxINhw7nEjyB0byBHT05FYcO5xI9i7p+IxIM=
w7lkxIfHnGbEk2phdmF4LmNyeXB0by5DaXBoZXLHnGbEk2XHmMSH

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。