南明离火
移动应用检测平台

ANDROID 静态分析报告

□□□□TV • v1.2.35

分析日期: 2025-04-26 21:03:36

i应用概览

文件名称:	□□□□TV v1.2.35.apk
文件大小:	28.02MB
应用名称:	□□□□TV
软件包名:	kr.co.yonhapnewstv.mobile
主活动:	kr.co.yonhapnewstv.mobile.SplashActivity
版本号:	1.2.35
最小SDK:	21
目标SDK:	34
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	54/100 (中风险)
杀软检测:	2 个杀毒软件报毒
MD5:	836e2fbf78f01539952d8fae63c31cdb
SHA1:	cedd4ea9d988433642a297290a[illegible]c30c7d846fb
SHA256:	300f5618239938125b4f69cbbdec8d244cf73609ee[illegible]570f8c2c20633de69e

分析结果严重性

高危	中危	信息	安全	关注
1	17	3	2	0

四大组件信息

Activity组件：11个，其中export的有：7个
Service组件：3个，其中export的有：1个
Receiver组件：1个，其中export的有：1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=KR, ST=Unknown, L=Seoul, O=YonhapnewsTV, OU=Unknown, CN=YonhapnewsTV
签名算法: rsassa_pkcs1v15
有效期自: 2016-02-19 01:51:09+00:00
有效期至: 2043-07-07 01:51:09+00:00
发行人: C=KR, ST=Unknown, L=Seoul, O=YonhapnewsTV, OU=Unknown, CN=YonhapnewsTV
序列号: 0x23c73aa1
哈希算法: sha256
证书MD5: b7121e1a309a0fa10eb70a09b1bb5bb9
证书SHA1: c1ab6e5da3de8000a43684cb8a9fd3fea0ed9c34
证书SHA256: afab0eb61f4b6a18445d9658975f8f30f9bfdfde93724460b658514682ea0326
证书SHA512:
d2d0efc1256193b66702eb89a29a1764d80c2c00cf959e91f4706b913a3cf7a3895af2a33272528caccdd1010f90e7e8eeaa7f5e[illegible]65778be51ad272e9650dc0

公钥算法: rsa
密钥长度: 2048
指纹: 29230a2cfa6dd3efed1cccb9a2b45b65696e78c75121ff14a23eba61208abfbd
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.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.POST_NOTIFICATIONS	危险	发送通知的运行时权限	允许应用发布通知，Android 13 引入的新权限。
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.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.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.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。
android.permission.WAKE_LOCK	危险	防止手机休眠	允许应用程序防止手机休眠，在手机屏幕关闭后后台进程仍然运行。
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。
com.google.android.c2dm.permission.RECEIVE	普通	接收推送通知	允许应用程序接收来自云的推送通知。

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: **0** | 警告: **11** | 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	应用程序数据可以被备份 [android:allowBackup=true]	警告	这个标志允许任何人通过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 (kr.co.yonhapnewstv.mobile.MainActivity) 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。
4	Activity (kr.co.yonhapnewstv.mobile.SubActivity) 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。
5	Activity (kr.co.yonhapnewstv.mobile.ReportActivity) 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 (kr.co.yonhapnewstv.mobile.SettingActivity) 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。
7	Activity (kr.co.yonhapnewstv.mobile.DummyPopActivity) 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 (kr.co.yonhapnewstv.mobile.push.NotiDummyActivity) 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。
9	Activity (kr.co.yonhapnewstv.mobile.GuideActivity) 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	Service (kr.co.yonhapnewstv.mobile.push.GCFirebaseMessagingService) 未被保护。 [android:exported=true]	警告	发现 Service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.google.firebase.iid.FirebaseInstanceIdReceiver) 受权限保护，但是应该检查权限的保护级别。 Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	警告	发现一个 Broadcast Receiver被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。

</> 安全漏洞检测

高危: **1** | 警告: **5** | 信息: **2** | 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	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	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
4	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
5	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
6	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

7	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
8	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

行为分析

编号	行为	标签	文件
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
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
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
00078	获取网络运营商名称	信息收集 电话服务	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
00033	查询IMEI号	信息收集	升级会员：解锁高级权限
00066	查询ICCID号码	信息收集	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
00036	从 res/raw 目录获取资源文件	反射	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
00121	创建目录	文件 命令	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
00054	从文件安装其他APK	反射	升级会员：解锁高级权限
00202	打电话	控制	升级会员：解锁高级权限

00203	将电话号码放入意图中	控制	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
00031	检查当前正在运行的应用程序列表	反射 信息收集	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.VIBRATE android.permission.CAMERA android.permission.WAKE_LOCK
其它常用权限	6/46	android.permission.INTERNET android.permission.READ_MEDIA_IMAGES android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE com.google.android.c2dm.permission.RECEIVE

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
kauth.kakao.com	安全	否	**IP地址:** 121.53.90.6 **国家:** 大韩民国 **地区:** 首尔teukbyeolsi **城市:** 首尔 **纬度:** 37.566311 **经度:** 126.977203 **查看:** Google 地图
app.yonhapnewstv.co.kr	安全	否	**IP地址:** 43.201.237.165 **国家:** 大韩民国 **地区:** 首尔teukbyeolsi **城市:** 首尔 **纬度:** 37.566311 **经度:** 126.977203 **查看:** Google 地图
accounts.kakao.com	安全	否	**IP地址:** 110.76.142.110 **国家:** 大韩民国 **地区:** 济州 **城市:** 济州 **纬度:** 33.513191 **经度:** 126.523346 **查看:** Google 地图

account.apple.com	安全	否	**IP地址:** 17.171.11.100 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 丘珀蒂诺 **纬度:** 37.316605 **经度:** -122.046486 **查看:** Google 地图
api.twitter.com	安全	否	**IP地址:** 121.53.90.6 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
nid.naver.com	安全	否	**IP地址:** 121.53.90.6 **国家:** 大韩民国 **地区:** 京畿道 **城市:** 城南市 **纬度:** 37.420624 **经度:** 127.126717 **查看:** Google 地图
yonhapnewstv-1223.firebaseio.com	安全	否	**IP地址:** 34.120.160.131 **国家:** 美国 **地区:** 密苏里州 **城市:** 堪萨斯城 **纬度:** 39.099731 **经度:** -94.578568 **查看:** Google 地图

URL链接分析

URL信息	源码文件
• javascript:setapplicationnotupdate	kr/co/yonhapnewstv/mobile/SubActivity.java
• javascript:setapplicationnotupdate	kr/co/yonhapnewstv/mobile/MainActivity.java
• https://app.yonhapnewstv.co.kr/ • https://www.facebook.com • https://kauth.kakao.com • https://app.yonhapnewstv.co.kr/bookmark/update • https://nid.naver.com • https://api.twitter.com • https://account.apple.com • https://app.yonhapnewstv.co.kr • https://app.yonhapnewstv.co.kr/live • https://app.yonhapnewstv.co.kr/app_version.txt • https://accounts.google.com • https://app.yonhapnewstv.co.kr/bookmark/check • https://accounts.kakao.com • https://app.yonhapnewstv.co.kr/yn/v1/search	kr/co/yonhapnewstv/mobile/Define.java
• javascript:setapplicationnotupdate	kr/co/yonhapnewstv/mobile/ReportActivity.java

• https://app.yonhapnewstv.co.kr/device/pushnotification • https://app.yonhapnewstv.co.kr/device/modpushnotification	kr/co/yonhapnewstv/mobile/network/tr/BaseUrl.java
• https://yonhapnewstv-1223.firebaseio.com	自研引擎-S

FIREBASE数据库分析

标题	严重程度	描述信息
应用与Firebase数据库通信	信息	该应用与位于 https://yonhapnewstv-1223.firebaseio.com 的 Firebase 数据库进行通信

Firebase远程配置已禁用	安全	Firebase远程配置URL （ https://firebaseremoteconfig.googleapis.com/v1/projects/1090551653553/namespaces/firebase:fetch?key=AIzaSyAL0A2HNN24m6rgKl-3ZYLXaA9EtB1v3N4 ） 已禁用。响应内容如下所示:
		{
		"state": "NO_TEMPLATE"
		}

第三方SDK

SDK名称	开发者	描述信息
Google Play Service	Google	借助 Google Play 服务，您的应用可以利用由 Google 提供的最新功能，例如地图，Google+ 等，并通过 Google Play 商店以 APK 的形式分发自动平台更新。 这样一来，您的用户可以更快地接收更新，并且可以更轻松地集成 Google 必须提供的最新信息。
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。
Firebase	Google	Firebase 提供了分析、数据库、消息传递和崩溃报告等功能，可助您快速采取行动并专注于您的用户。
Jetpack Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。

密钥凭证

可能的密钥
"firebase_database_url" : "https://yonhapnewstv-1223.firebaseio.com"
"google_api_key" : "AIzaSyAL0A2HNN24m6rgKl-3ZYLXaA9EtB1v3N4"
"google_app_id" : "1:1090551653553:android:924f208f843866a6"
"google_crash_reporting_api_key" : "AIzaSyAL0A2HNN24m6rgKl-3ZYLXaA9EtB1v3N4"

GooglePlay应用信息

标题: □□□□ TV

评分: 4.03 **安装:** 100,000+ **价格:** 0 **Android版本支持:** **分类:** 新闻杂志 **Play Store URL:** kr.co.yonhapnewstv.mobile

开发者信息: YONHAPNEWS TV, YONHAPNEWS+TV, None, None, genie@yna.co.kr,

发布日期: 2016年2月18日 **隐私政策:** Privacy link

关于此应用:

韩国新闻的开端，韩联社新闻电视台，24小时新闻频道 值得信赖的广播、差异化广播、与观众一起广播、全球新闻频道！ 立即免费查看韩联社新闻电视应用程序，该应用程序可提供真实的实时新闻和现场突发新闻。 【主要特点】 • 随时随地观看24小时实时新闻。 • 我们实时提供各个领域的新闻，包括政治、经济、社会、体育、文化/娱乐、地区、世界和天气。 • 您捕捉到的瞬间就是新闻。通过报告轻松参与。 [报告] • 可以看到[Dadarul采访]、[现场问题]、[彩伊的生活场景]、[热血D]等数字原创节目中未曾见过的有趣新闻。 • News Focus、News 1st Street 和 News Watch 节目也以音频新闻形式提供。 • 您可以使用书签功能保存新闻以便稍后查看。 • 支持深色模式，更护眼。 • 所有文章均可在Facebook、X、KakaoTalk、Naver 等各种社交平台上分享。 [可选的访问权限信息] - 相机、照片存储：举报时需要附加设备上保存的照片和视频。 ※ 如果拒绝选择权，则服务的使用可能会受到限制，但可以使用其他服务。 如果您在使用应用程序时遇到任何不便或服务需要改进，请将您的反馈发送至以下联系方式。这对于提供更好的服务将非常有帮助。 负责韩联社新闻电视应用程序服务的电子邮件： genie@yna.co.k

---

免责声明及风险提示: