南明离火
移动应用检测平台

ANDROID 静态分析报告

load_html • v1.0

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: 2025-07-07 15:21:47

应用概览

文件名称:	题15-18.apk
文件大小:	4.34MB
应用名称:	load_html
软件包名:	com.nosugar.loadhtml
主活动:	com.nosugar.loadhtml.MainActivity
版本号:	1.0
最小SDK:	24
目标SDK:	24
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	28/100 (重大风险)
杀软检测:	AI评估：安全
MD5:	e887ac9b8e46200c727bc0a907e68cef
SHA1:	320ddedc1b0aa008a0b0318956e6ff44f320dea3
SHA256:	d61363b5d9ead4bf04f10790a61e5025d6a35f9a9f7dc3a4be750c4e5c9e377d

分析结果严重性分布

高危	中危	信息	安全	关注
4	1	0	1	0

四大组件导出状态统计

Activity组件：1个，其中export的有： 0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

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

应用签名证书信息

APK已签名
v1 签名: False
v2 签名: True
v3 签名: False
v4 签名: False
主题: CN=Android Debug, O=Android, C=US
签名算法: rsassa_pkcs1v15
有效期自: 2022-04-02 07:30:03+00:00
有效期至: 2052-03-25 07:30:03+00:00
发行人: CN=Android Debug, O=Android, C=US
序列号: 0x1
哈希算法: sha1
证书MD5: 7a846db167898f2f5160b475e38b536d
证书SHA1: 5f00c034f2877ee35cd93ed8b6e181fc2162db1f
证书SHA256: e73f8a677e2cb1bf77df7997ec1feb5468f7997b93690321378c7b560b594b5f
证书SHA512:
7f8e8c18bc71c58ff3e6f44b18718371d6b037ec12e740996aa9f4c80e5aafc0b6b3ec977439d42788c902[illegible]0a352447cfd2010593410[illegible]5f40247e41c22b

公钥算法: rsa
密钥长度: 2048
指纹: 29b26f48fa8949c30d33598173ee108191a9068071a7bb784446ea5ffd41d864
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。

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: **1** | 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。
检测到调试证书签名	高危	检测到应用使用调试证书签名。请勿在生产环境中使用调试证书。

Manifest 配置安全分析

高危: **2** | 警告: **1** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息

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

1	应用可被调试 [android:debuggable=true]	高危	应用开启了可调试标志，攻击者可轻易附加调试器进行逆向分析，导出堆栈信息或访问调试相关类，极大提升被攻击风险。
2	应用数据允许备份 [android:allowBackup=true]	警告	该标志允许通过 adb 工具备份应用数据。启用 USB 调试的用户可直接复制应用数据，存在数据泄露风险。
3	Activity (com.nosugar.loadhtml.MainActivity) 易受 StrandHogg 2.0 攻击	高危	检测到 Activity 存在 StrandHogg 2.0 任务劫持漏洞。攻击者可将恶意 Activity 置于易受攻击应用的任务栈顶部，使应用极易成为钓鱼攻击目标。可通过将启动模式设置为 "singleInstance" 并将 taskAffinity 设为空（taskAffinity=""），或将应用的 target SDK 版本（24）升级至 28 及以上，从平台层面修复该漏洞。

代码安全漏洞检测

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

序号	问题	等级	参考标准	文件位置
1	启用了调试配置。生产版本不能是可调试的	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

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	0/30	
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
kltdi.cn	安全	否	No Geolocation information available.

URL 链接安全分析

URL信息	源码文件

本报告由南明离火移动安全分析平台生成

• https://www.baidu.com	自研引擎-A
• https://kltdi.cn	com/nosugar/loadhtml/MainActivity.java

第三方 SDK 组件分析

SDK名称	开发者	描述信息
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

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，不构成任何投资意见或建议。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。

© 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