南明离火
移动应用检测平台

ANDROID 静态分析报告

SPAIN TV+ • v2.14.8

分析日期: 2024-03-09 14:29:43

应用概览

文件名称:	SpainTV-APK-v2.14.8-ModFYP.apk
文件大小:	8.15MB
应用名称:	SPAIN TV+
软件包名:	com.mcdstore.spaintv
主活动:	com.mcdstore.spaintv.MainActivity
版本号:	2.14.8
最小SDK:	19
目标SDK:	29
加固信息:	未加壳
应用程序安全分数:	42/100 (中风险)
跟踪器检测:	1/432
杀软检测:	3 个杀毒软件报毒
MD5:	fb654ec376ec94e584d29f71bc1f6f4b
SHA1:	112c59bb76746207bb55c5f8632b78fa39e0a944
SHA256:	6aea5be919ff50aefbb06d7d60d2afa3a286ea3812a2e78d3f9543ba02593e7

分析结果严重性分布

高危	中危	信息	安全	关注
5	18	1	1	0

四大组件导出状态统计

Activity组件：8个，其中export的有：3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：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=CO, ST=Antioquia, L=Medellin, O=MCD Technology Apps, OU=Systems Engineer, CN=Mark Castillo Oficial
签名算法: rsassa_pkcs1v15
有效期自: 2023-08-16 02:31:50+00:00
有效期至: 2204-07-03 02:31:50+00:00
发行人: C=CO, ST=Antioquia, L=Medellin, O=MCD Technology Apps, OU=Systems Engineer, CN=Mark Castillo Oficial
序列号: 0x25002395
哈希算法: sha256
证书MD5: 28bc8ae7e9d252f40cb439f96e13f50f
证书SHA1: ecc6c2c5b01156802b38300dc91d2f30046263ef
证书SHA256: 7b111fbaf44935b908c8a858c7de6f21adfa7d19ea1a1621d63be77ad1e16801
证书SHA512:
845b38df0639202cbe455be987662c7c730c60481651174fb8106108b3a3ccb62edd0650adf2e7962c8f0d0d111aaeed1b11cc86[illegible]ed2f37721808b90935587

公钥算法: rsa
密钥长度: 2048
指纹: 7e9f6d5fdc956584a4a6ce197b6b0814e28b379dd0715b9d30cff4b0fce4ad2d
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_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.RECEIVE_BOOT_COMPLETED	普通	开机自启	允许应用程序在系统完成启动后即自行启动。这样会延长手机的启动时间，而且如果应用程序一直运行，会降低手机的整体速度。
android.permission.FOREGROUND_SERVICE	普通	创建前台Service	Android 9.0以上允许常规应用程序使用 Service.startForeground，用于podcast播放（推送悬浮播放，锁屏播放）
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。
com.mcdstore.spaintv_com.google.android.gms.permission.AD_ID	未知	未知权限	来自 android 引用的未知权限。
com.mcdstore.spaintv.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.mcdstore.spaintv.MainActivity	Schemes: http://, https://, content://, asset://, file://, Hosts: *, Path Patterns: .*\\.exolist\\.json,
com.google.firebase.auth.internal.GenericIdpActivity	Schemes: genericidp://, Hosts: firebase.auth, Paths: /,

com.google.firebase.auth.internal.RecaptchaActivity	Schemes: recaptcha://, Hosts: firebase.auth, Paths: /,

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
应用程序存在Janus漏洞	警告	应用程序使用了v1签名方案进行签名，如果只使用v1签名方案，那么它就容易受到安卓5.0-8.0上的Janus漏洞的攻击。在安卓5.0-7.0上运行的使用了v1签名方案的应用程序，以及同时使用了v2/v3签名方案的应用程序也同样存在漏洞。

Manifest 配置安全分析

高危: **2** | 警告: **9** | 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 4.4-4.4.4, [minSdk=19]	警告	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。
3	Activity (com.mcdstore.spaintv.AdultsActivity) 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，因此使其对设备上的任何其他应用程序都可访问。
4	Activity (com.mcdstore.spaintv.PelisActivity) 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，因此使其对设备上的任何其他应用程序都可访问。
5	Activity (com.mcdstore.spaintv.PlayerActivity) 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，因此使其对设备上的任何其他应用程序都可访问。

6	Service (com.google.android.tvonline.scheduler.PlatformScheduler$PlatformSchedulerService) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	警告	发现一个 Service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。
7	Activity (com.google.firebase.auth.internal.GenericIdpActivity) 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。
8	Activity (com.google.firebase.auth.internal.GenericIdpActivity) 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，因此使其对设备上的任何其他应用程序都可访问。
9	Activity (com.google.firebase.auth.internal.RecaptchaActivity) 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。
10	Activity (com.google.firebase.auth.internal.RecaptchaActivity) 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，因此使其对设备上的任何其他应用程序都可访问。
11	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.DUMP [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。

代码安全漏洞检测

高危: **3** | 警告: **6** | 信息: **1** | 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
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	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

4	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
5	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
6	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
7	SSL的不安全实现。信任所有证书或接受自签名证书是一个关键的安全漏洞。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
8	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
9	应用程序在加密算法中使用ECB模式。ECB模式是已知的弱模式，因为它对相同的明文块[UNK]产生相同的密文	高危	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-2	升级会员：解锁高级权限
10	应用程序创建临时文件。敏感信息永远不应该被写进临时文件	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
11	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

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）	FORTIFY(常用函数加强检查)	SYMBOLSSTRIPPED(裁剪符号表)
1	arm64-v8a/libnpdcc.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。		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: ['__strlen_chk', '__memmove_chk', '__vsnprintf_chk']	False warning 符号可用
2	arm64-v8a/libtbsp-jni.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。		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: ['__strrchr_chk', '__vsnprintf_chk', '__memcpy_chk', '__strchr_chk', '__vsprintf_chk', '__strncpy_chk']	False warning 符号可用

敏感权限滥用分析

类型	匹配	权限

本报告由南明离火移动安全分析平台生成

恶意软件常用权限	2/30	android.permission.RECEIVE_BOOT_COMPLETED android.permission.READ_PHONE_STATE
其它常用权限	4/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.READ_EXTERNAL_STORAGE android.permission.FOREGROUND_SERVICE

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
www.recaptcha.net	安全	否	**IP地址:** 142.250.188.227 **国家:** United States of America **地区:** California **城市:** Mountain View **纬度:** 37.405991 **经度:** -122.078514 **查看:** Google 地图
exoplayer.dev	安全	否	**IP地址:** 185.199.109.153 **国家:** United States of America **地区:** Pennsylvania **城市:** California **纬度:** 40.065632 **经度:** -79.891708 **查看:** Google 地图
googleads.g.doubleclick.net	安全	否	**IP地址:** 142.250.176.2 **国家:** United States of America **地区:** California **城市:** Mountain View **纬度:** 37.405991 **经度:** -122.078514 **查看:** Google 地图
www.gstatic.com	安全	否	**IP地址:** 142.250.72.163 **国家:** United States of America **地区:** California **城市:** Mountain View **纬度:** 37.405991 **经度:** -122.078514 **查看:** Google 地图
pagead2.googlesyndication.com	安全	否	**IP地址:** 172.217.12.130 **国家:** United States of America **地区:** Virginia **城市:** Ashburn **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图

aomedia.org	安全	否	**IP地址:** 185.199.109.153 **国家:** United States of America **地区:** Pennsylvania **城市:** California **纬度:** 40.065632 **经度:** -79.891708 **查看:** Google 地图
schemas.microsoft.com	安全	否	**IP地址:** 13.107.213.74 **国家:** United States of America **地区:** Washington **城市:** Redmond **纬度:** 47.682899 **经度:** -122.120903 **查看:** Google 地图
dashif.org	安全	否	**IP地址:** 185.199.109.153 **国家:** United States of America **地区:** Pennsylvania **城市:** California **纬度:** 40.065632 **经度:** -79.891708 **查看:** Google 地图
www.dom.com	安全	否	**IP地址:** 15.60.233.28 **国家:** United States of America **地区:** California **城市:** Redwood City **纬度:** 37.532440 **经度:** -122.248833 **查看:** Google 地图
admob-gmats.uc.r.appspot.com	安全	否	**IP地址:** 172.217.12.148 **国家:** United States of America **地区:** Virginia **城市:** Ashburn **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
eventos-py-dc80c-default-rtdb.firebaseio.com	安全	否	**IP地址:** 34.120.160.131 **国家:** United States of America **地区:** Missouri **城市:** Kansas City **纬度:** 39.099731 **经度:** -94.578568 **查看:** Google 地图
www.markcastilloficial.com	安全	否	**IP地址:** 104.21.51.47 **国家:** United States of America **地区:** California **城市:** San Francisco **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• http://ns.adobe.com/xap/1.0/	c3/a.java

• https://www.markcastilloficial.com/mcdstore_applications/TVOnline/movies.php	com/mcdstore/spaintv/PelisActivity.java
• https://exoplayer.dev/issues/player-accessed-on-wrong-thread	m2/e1.java
• https://aomedia.org/emsg/ID3 • https://developer.apple.com/streaming/emsg-id3	m3/a.java
• https://console.firebase.google.com/.	o5/m.java
• http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense	r2/l0.java
• https://firebase.google.com/docs/database/ios/structure-data#best_practices_for_data_structure • https://firebase.google.com/docs/database/android/retrieve-data#filtering_data • https://github.com/firebase/firebase-android-sdk	t5/c.java
• https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps	u0/b.java
• https://exoplayer.dev/issues/cleartext-not-permitted	v4/a0.java
• http://dashif.org/guidelines/last-segment-number • data:cs:AudioPurposeCS:2007 • http://dashif.org/guidelines/trickmode	y3/d.java
• https://aomedia.org/emsg/ID3 • http://localhost • https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/production/mraid/v3/mraid_app_expanded_banner.js • http://ns.adobe.com/xap/1.0/ • www.googleapis.com/identitytoolkit/v3/relyingparty • http://www.dom.com/path? • www.gstatic.com/recaptcha • data:cs:AudioPurposeCS:2007 • https://eventos-py-dc80c-default-rtdb.firebaseio.com • https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/native_ads.html • https://imasdk.googleapis.com/native/sdkloader/native_sdk_v3_debug.html • https://exoplayer.dev/issues/cleartext-not-permitted • https://www.recaptcha.net/recaptcha/api3 • https://imasdk.googleapis.com/admob/sdkloader/native_video.html • http://dashif.org/guidelines/last-segment-number • https://exoplayer.dev/issues/player-accessed-on-wrong-thread • https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/production/mraid/v3/mraid_app_banner.js • https://developer.android.com/google/play/integrity/reference/com/google/android/play/core/integrity/model/IntegrityErrorCode.html# • www.recaptcha.net • https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/production/sdk-core-v40-impl.html • data:enabled • https://admob-gmats-uc.r.appspot.com/ • https://googleads.g.doubleclick.net • https://pagead2.googlesyndication.com/pagead/ping?e=2&f=1 • https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps • http://dashif.org/guidelines/trickmode • https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/production/mraid/v3/mraid_app_interstitial.js • javascript:adsense.mobileads.afmanotify.receiveMessage • https://imasdk.googleapis.com/native/sdkloader/native_sdk_v3.html • https://developer.apple.com/streaming/emsg-id3 • https://www.markcastilloficial.com/mcdstore_applications/TVOnline/movies.php • http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense • https://plus.google.com/	自研引擎分析结果

Firebase 配置安全检测

标题	严重程度	描述信息

第三方 SDK 组件分析

SDK名称	开发者	描述信息
Google Play Service	Google	利用 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。
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。
Picasso	Square	一个强大的 Android 图片下载缓存库。
Jetpack ProfileInstaller	Google	让库能够提前预填充要由 ART 读取的编译轨迹。

邮箱地址敏感信息提取

EMAIL	源码文件
u0013android@android.com0 u0013android@android.com	z0/b0.java
android@android.com0	自研引擎分析结果

第三方追踪器检测

名称	类别	网址
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312

敏感凭证泄露检测

可能的密钥
"google_api_key" : "AIzaSyBMnrsqsqtHS8wgrrjTMzlbKxqoKQsZgDU"
"google_crash_reporting_api_key" : "AIzaSyBMnrsqsqtHS8wgrrjTMzlbKxqoKQsZgDU"
"firebase_database_url" : "https://eventos-py-dc80c-default-rtdb.firebaseio.com"
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
9a04f079-9840-4286-ab92-e65be0885f95
e2719d58-a985-b3c9-781a-b030af78d30e
16a09e667f3bcc908b2fb1366ea957d3e3ade[illegible]75099da2f590b06673[illegible]a

免责声明及风险提示: