



ANDROID 静态分析报告



📱 CDE Smartband • v25.1.0

分析日期: 2025-07-06 10:39:30

i应用概览

文件名称:	CDE Smartband v25.1.0.apk
文件大小:	35.86MB
应用名称:	CDE Smartband
软件包名:	com.cdelightband.smarthome
主活动:	com.cdelightband.smarthome.ui.loginregconfig.Splash
版本号:	25.1.0
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:	49/100 (中风险)
跟踪器检测:	3/432
杀软检测:	经检测，该文件安全
MD5:	1781e97bec1360a7016a8a8b32dd0f17
SHA1:	a044a0b3c5dc94d171d1cc17f52af582284ddced7
SHA256:	9c9eac12f0f1be907c696e864bb89b3d0ebf308aaad86c0b292f2cd6ac081aaaa

📊 分析结果严重性分布

🚨 高危	⚠️ 中危	i 信息	✓ 安全	🔍 关注
3	17	1	2	2

📦 四大组件导出状态统计

Activity组件: 5个, 其中export的有: 5个
Service组件: 11个, 其中export的有: 0个
Receiver组件: 4个, 其中export的有: 2个
Provider组件: 4个, 其中export的有: 0个

应用签名证书信息

APK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=Google Inc., OU=Android, CN=Android

签名算法: rsassa_pkcs1v15

有效期自: 2022-09-07 06:03:28+00:00

有效期至: 2052-09-07 06:03:28+00:00

发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android

序列号: 0x8febdbb65d60bd702f22aaf5950378cc3ccc1ac7

哈希算法: sha256

证书MD5: 9d41d39596ab69b386864993aa74f5d0

证书SHA1: 58013039367f142739afc75b02962d1179177800

证书SHA256: 92c9c7860b519e3dcc3f7d067753e5cd68ec289321d7a6b1a9502932a3c04c92

证书SHA512: e443d90bae08cc3b453c29edd2c8662b28537b1e1e957a51a1567e4fad29b0440f8841bfa58f3efe8ebc0eafcf3d96472a6403772a37b07864762acc58c3048

公钥算法: rsa

密钥长度: 4096

指纹: 661adb0acb157b16b793aeb80d1a0ddb0a8f1ab2ab07aa53ecfb17b8f6a14e6

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.USE_FINGERPRINT	普通	允许使用指纹	此常量在 API 级别 28 中已弃用。应用程序应改为请求USE_BIOMETRIC
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_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.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.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_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.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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
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.RECEIVE_BOOT_COMPLETE D	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.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。
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。
com.google.android.gms.permission.AD_ID	普通	应用程序显示广告	此应用程序使用 Google 广告 ID，并且可能会投放广告。
android.permission.ACCESS_AD SERVICES_ATTRIBUTION	普通	允许应用程序访问广告服务归因	这使应用能够检索与广告归因相关的信息，这些信息可用于有针对性的广告目的。应用程序可以收集有关用户如何与广告互动的数据，例如点击或展示，以衡量广告活动的有效性。
android.permission.ACCESS_AD SERVICES_AD_ID	普通	允许应用访问设备的广告 ID。	此 ID 是 Google 广告服务提供的唯一、用户可重置的标识符，允许应用出于广告目的跟踪用户行为，同时维护用户隐私。
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	普通	Google 定义的权限	由 Google 定义的自定义权限。
android.permission.REORDER_TASKS	危险	对正在运行的应用程序重新排序	允许应用程序将任务移至前端和后台。恶意应用程序可借此强行进入前端，而不受您的控制。
com.cdelightband.smarthome.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
sdk.pendo.io.activities.PendoGateActivity	Schemes: pendo-3980b6d1://,
com.amazon.identity.auth.device.workflow.WorkflowActivity	Schemes: amzn://, Hosts: com.cdelightband.smarthome,

网络通信安全风险分析

高危: 1 | 警告: 0 | 信息: 0 | 安全: 0

序号	范围	严重级别	描述
1	*	高危	基本配置不安全地配置为允许到所有域的明文流量。

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: 7 | 信息: 0 | 屏蔽: 0

序号	问题	严重程度	描述信息
1	应用已配置网络安全策略 [android:networkSecurity Config=@xml/network_se curity_config]	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。
2	Activity (sdk.pendo.io.acti vities.PendoGateActivity) 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。
3	Activity (com.amazon.iden tity.auth.device.workflow. WorkflowActivity) 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	Broadcast Receiver (com. google.firebase.iid.Fireba seInstanceIdReceiver) 受 权限保护，但应检查权限保 护级别。 Permission: com.google.a ndroid.c2dm.permission.S END [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受未在本应用定义的权限保护。请在权 限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并 与组件交互；若为 signature，仅同证书签名应用可访问。
5	Activity (androidx.test.cor e.app.InstrumentationActi vityInvoker\$BootstrapActi vity) 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。
6	Activity (androidx.test.cor e.app.InstrumentationActi vityInvoker\$EmptyActivity) 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。
7	Activity (androidx.test.cor e.app.InstrumentationActi vityInvoker\$EmptyFloatin gActivity) 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。
8	Broadcast Receiver (and roidx.profileinstaller.Profil eInstallReceiver) 受权限保 护，但应检查权限保护级别 。 Permission: android.perm ission.DUMP [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受未在本应用定义的权限保护。请在权 限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并 与组件交互；若为 signature，仅同证书签名应用可访问。

代码安全漏洞检测

高危: 2 | 警告: 8 | 信息: 1 | 安全: 1 | 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 Engineerin OWASP MASVS: MSTG-STORAGE-14	升级会员: 解锁高级权限
2	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
3	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
4	应用程序创建临时文件。敏感信息永远不应该被写入临时文件	警告	CWE: CWE-276: 默认权限不正确 OWASP Top 10: M2: I nsecure Data Storag e OWASP MASVS: MSTG-STORAGE-2	升级会员: 解锁高级权限
5	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
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: I nsufficient Cryptogr apy 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: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: I nsufficient Cryptogr aphy OWASP MASVS: MSTG-CRYPTO-4	升级会员: 解锁高级权限
8	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: I nsecure Data Storag e OWASP MASVS: MSTG-STORAGE-2	升级会员: 解锁高级权限

9	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
10	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
11	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
12	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	高危	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） OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-6	升级会员：解锁高级权限

应用行为分析

编号	行为	标签	文件
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
00130	获取当前WiFi信息	WiFi 信息收集	升级会员：解锁高级权限
00047	查询本地IP地址	网络 信息收集	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
00051	通过IntentData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
00013	读取文件并将其放入流中	文件	升级会员：解锁高级权限
00012	读取数据并放入缓冲流	文件	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

00162	创建 InetAddress 对象并连接到它	socket	升级会员：解锁高级权限
00163	创建新的 Socket 并连接到它	socket	升级会员：解锁高级权限
00026	方法反射	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
00191	获取短信收件箱中的消息	短信	升级会员：解锁高级权限
00189	获取短信内容	短信	升级会员：解锁高级权限
00188	获取短信地址	短信	升级会员：解锁高级权限
00200	从联系人列表中查询数据	信息收集 联系人	升级会员：解锁高级权限
00201	从通话记录中查询数据	信息收集 通话记录	升级会员：解锁高级权限
00077	读取敏感数据（短信、通话记录等）	信息收集 短信 通话记录	升级会员：解锁高级权限
00019	从给定的类名中查找方法，通常用于反射	反射	升级会员：解锁高级权限
00183	获取当前相机参数并更改设置	相机	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
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
00024	Base64解码后写入文件	反射 文件	升级会员：解锁高级权限
00004	获取文件名并将其放入 JSON 对象	文件 信息收集	升级会员：解锁高级权限
00114	创建到代理地址的安全套接字连接	网络 命令	升级会员：解锁高级权限
00123	连接到远程服务器后将响应保存为 JSON	网络 命令	升级会员：解锁高级权限
00029	动态初始化类对象	反射	升级会员：解锁高级权限

00157	使用反射实例化新对象，可能用于 dexClassLoader	反射 dexClassLoad er	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	4/30	android.permission.WAKE_LOCK android.permission.RECORD_AUDIO android.permission.CAMERA android.permission.RECEIVE_BOOT_COMPLETED
其它常用权限	10/46	android.permission.INTERNET android.permission.ACCESS_WIFI_STATE android.permission.ACCESS_NETWORK_STATE android.permission.CHANGE_WIFI_STATE android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE com.google.android.c2dm.permission.RECEIVE com.google.android.gms.permission.AD_ID com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE android.permission.REORDER_TASKS

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
ktor.io	安全	否	IP地址: 13.249.126.87 国家: 美国 地区: 佐治亚州 城市: 亚特兰大 纬度: 33.748795 经度: -84.387543 查看: Google 地图
data.pendo.io	安全	否	IP地址: 98.82.160.170 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

youtrack.jetbrains.com	安全	否	IP地址: 13.249.126.87 国家: 爱尔兰 地区: 都柏林 城市: 都柏林 纬度: 53.344151 经度: -6.267249 查看: Google 地图
data.eu.pendo.io	安全	否	IP地址: 98.82.160.170 国家: 美国 地区: 密苏里州 城市: 堪萨斯城 纬度: 39.099731 经度: -94.578368 查看: Google 地图
api.amazon.com	安全	否	IP地址: 98.82.160.170 国家: 美国 地区: 弗吉尼亚州 城市: 阿什本 纬度: 39.039474 经度: -77.491106 查看: Google 地图
cloud-devfunc.calix.com	安全	否	IP地址: 65.35.30.167 国家: 美国 地区: 俄勒冈 城市: 波特兰 纬度: 45.523460 经度: -122.676468 查看: Google 地图
cloud-stg.calix.com	安全	否	IP地址: 52.13.140.158 国家: 美国 地区: 俄勒冈 城市: 波特兰 纬度: 45.523460 经度: -122.676468 查看: Google 地图
app.pendo	安全	否	No Geolocation information available.
itunes.apple.com	安全	是	IP地址: 117.66.45.139 国家: 中国 地区: 安徽 城市: 马鞍山市 纬度: 31.695681 经度: 118.498253 查看: 高德地图
calixcloud-ca.calix.com	安全	否	IP地址: 3.97.30.171 国家: 加拿大 地区: 魁北克 城市: 蒙特利尔 纬度: 45.508839 经度: -73.587807 查看: Google 地图

cdelightband.com	安全	否	IP地址: 18.224.102.87 国家: 美国 地区: 俄亥俄州 城市: 哥伦布 纬度: 39.961380 经度: -82.997749 查看: Google 地图
devfunc-rgw.calix.com	安全	否	IP地址: 13.249.126.87 国家: 美国 地区: 俄勒冈 城市: 波特兰 纬度: 45.523460 经度: -122.676468 查看: Google 地图
data.jpnpendo.io	安全	否	IP地址: 34.149.195.87 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
adsd.asd	安全	否	No Geolocation information available.
us1.data.pendo.io	安全	否	IP地址: 34.110.177.118 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
api.calix.ai	安全	否	IP地址: 35.185.254.173 国家: 美国 地区: 俄勒冈 城市: 达尔斯 纬度: 45.594784 经度: -121.178688 查看: Google 地图
cloud-dev.calix.com	安全	否	IP地址: 54.69.217.11 国家: 美国 地区: 俄勒冈 城市: 波特兰 纬度: 45.523460 经度: -122.676468 查看: Google 地图
rgw.ca.calix.com	安全	否	IP地址: 15.223.111.87 国家: 加拿大 地区: 魁北克 城市: 蒙特利尔 纬度: 45.508839 经度: -73.587807 查看: Google 地图

stage.api.calix.ai	安全	否	IP地址: 34.54.155.27 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
rgw.calix.ai	安全	否	IP地址: 54.200.64.227 国家: 美国 地区: 俄勒冈 城市: 波特兰 纬度: 45.523460 经度: -122.676468 查看: Google 地图
www.calix.com	安全	否	IP地址: 151.101.131.10 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
www.speedtest.net	安全	否	IP地址: 104.17.147.22 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
apps.apple.com	安全	是	IP地址: 220.177.176.9 国家: 中国 地区: 江西 城市: 吉安 纬度: 27.117161 经度: 114.979271 查看: 高德地图
data.hsbc.pendora	安全	否	IP地址: 34.54.104.198 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
dev.rgw.calix.ai	安全	否	IP地址: 162.255.119.170 国家: 美国 地区: 俄勒冈 城市: 波特兰 纬度: 45.523460 经度: -122.676468 查看: Google 地图

me.servifycare.com	安全	否	IP地址: 151.101.131.10 国家: 美国 地区: 弗吉尼亚州 城市: 阿什本 纬度: 39.039474 经度: -77.491806 查看: Google 地图
another.com	安全	否	IP地址: 162.255.119.170 国家: 美国 地区: 佐治亚州 城市: 亚特兰大 纬度: 33.727291 经度: -84.425377 查看: Google 地图
dev.api.calix.ai	安全	否	IP地址: 34.54.130.14 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
calixcloud.calix.com	安全	否	IP地址: 31.209.194.226 国家: 美国 地区: 俄勒冈 城市: 波特兰 纬度: 45.523460 经度: -122.676468 查看: Google 地图
stage.rgw.calix.ai	安全	否	IP地址: 35.80.220.209 国家: 美国 地区: 俄勒冈 城市: 波特兰 纬度: 45.523460 经度: -122.676468 查看: Google 地图

🌐 URL 链接安全分析

URL信息	源码文件
• https://www.calix.com/pages/ppi/conn-andiq-privacy-policy.html	自研引擎-A
• https://dev.rgw.calix.ai/map/v1/mobile/	com/calix/storage/StorageConstants.java
• http://127.0.0.1/	external/sdk/pendo/io/mozilla/javascript/tools/debugger/Dim.java

• https://data.jpn.pendo.io • https://data.eu.pendo.io • https://app.pendo.io • https://us1.data.pendo.io • https://data.hsbc.pendo.io • https://data.pendo.io	sdk/pendo.io/p8/b.java
• http://adsd.asd	com/calix/alertsui/compose/AlertDetailsUiKt.java
• https://rgw.calix.ai/map/v1/mobile/ • https://devfunc-rgw.calix.com/map/v1/mobile/ • https://stage.rgw.calix.ai/map/v1/mobile/	com/calix/settingsui/activities/SettingsActivity.java
• http://docs.google.com/gview?embedded=true&url=	com/cdelightband/smarthome/ui/settings/termsConditions.java
• http://javax.xml.xmlconstants/property/accessexternalstylesheet • http://javax.xml.xmlconstants/property/accessexternaldtd • http://javax.xml.xmlconstants/feature/secure-processing	external/sdk/pendo.io/mozilla/javascript/xmlimpl/XMLProcessor.java
• 2.5.1.1	sdk/pendo.io/s3/a.java
• http://docs.google.com/gview?embedded=true&url=	com/cdelightband/smarthome/ui/settings/PrivacyPolicy.java
• https://ktor.io/docs/http-client-engines.html	io/ktor/client/HttpClientJvmKt.java
• 2.5.4.8 • 2.5.4.3 • 2.5.4.41 • 2.5.4.97 • 2.5.4.7 • 2.5.4.20 • 2.5.4.6 • 2.5.4.11 • 2.5.4.10	sdk/pendo.io/e4/k.java

• 2.5.29.31 • 2.5.29.28 • 2.5.29.29 • 2.5.29.24 • 2.5.29.9 • 2.5.29.33 • 2.5.29.56 • 2.5.29.18 • 2.5.29.21 • 2.5.29.27 • 2.5.29.37 • 2.5.29.60 • 2.5.29.19 • 2.5.29.23 • 2.5.29.46 • 2.5.29.14 • 2.5.29.55 • 2.5.29.30 • 2.5.29.20 • 2.5.29.32 • 2.5.29.15 • 2.5.29.17 • 2.5.29.16 • 2.5.29.54 • 2.5.29.36 • 2.5.29.35	sdk/pendo.io/e/d/java
• https://youtrack.jetbrains.com/issue/ktor-6630/migrate-to-new-kotlinx-io-library	io/ktor/utils/io/DeprecationKt.java
• https://play.google.com/store/apps/details?id=com.amazon.dee.app	com/cdelightband/smarthome/ui/dashboard/ThingsToTryAlexa.java
• 1.3.36.3	sdk/pendo.io/b4/b.java
• 1.3.132.1	sdk/pendo.io/a4/b.java
• https://data.apn.pendo.io • https://data.eu.pendo.io • https://us1.data.pendo.io • https://data.hsbc.pendo.io • https://data.pendo.io	sdk/pendo.io/h9/b0.java

- https://apps.apple.com/in/app/arlo/id1459289784 - https://play.google.com/store/apps/details?id=com.arlo.app&hl=en_in&gl=us	com/cdelightband/smarthome/v4/ui/arlo/ArloListOfCameras.java
8.8.8.8 224.0.0.251	com/koushikdutta/async/dns/Dns.java
https://ktor.io/docs/migrating-2.html#serialization-client	io/ktor/client/plugins/json/JsonSerializer.java
https://ktor.io/docs/migrating-2.html#serialization-client	io/ktor/client/plugins/json/JsonPluginKt.java
- https://play.google.com/store/apps/details?id=servifycare.consumer.android&hl=en_us&gl=us - https://me.servifycare.com/login	com/cdelightband/smarthome/v4/ui/servify/Servify.java
- https://cloud-dev.calix.com/login - https://dev.api.calix.ai/v1/ - https://cloud-devfunc.calix.com/login - https://stage.api.calix.ai/v1/ - https://cloud-stg.calix.com/login - https://calixcloud-ca.calix.com/login - https://api.calix.ai/v1/ - https://calixcloud.calix.com/login	com/cdelightband/smarthome/environments/EnvironmentsModel.java
http://docs.google.com/gview?embedded=true&url=	com/cdelightband/smarthome/ui/settings/About.java
http://docs.google.com/gview?embedded=true&url=	com/calix/settingsui/viewmodels/AboutViewModel.java
2.5.29.35	sdk/pendo/io/j/b.java
https://play.google.com/store/apps/details?id=com.amazon.dee.app	com/cdelightband/smarthome/v5/V5TrywithAlexa.java
https://ktor.io/docs/migrating-2.html#serialization-client	io/ktor/client/plugins/json/JsonPlugin.java
https://api.amazon.com/auth/oz/token	com/cdelightband/smarthome/utils/AppConstants.java
- https://stage.rgw.calix.ai - https://play.google.com/store/apps/details?id=com.ciqpro.smarthome - https://dev.rgw.calix.ai - https://play.google.com/store/apps/details?id=com.samsung.android.oneconnect - https://devfunc-rgw.calix.com - https://rgw.calix.ai - http://docs.google.com/gview?embedded=true&url=	com/cdelightband/smarthome/utils/DialogManager.java
192.168.1.1 192.168.0.100	com/calix/networkui/compose/SatThinningDetailsUiKt.java

2.5.4.3 2.5.29.37 2.5.29.19 2.5.29.15 2.5.4.11 2.5.4.6 2.5.29.17 2.5.4.10	io/ktor/network/tls/OID.java
- https://dev.api.calix.ai/ - https://stage.rgw.calix.ai - https://dev.rgw.calix.ai - https://cloud-dev.calix.com/login - https://rgw.ca.calix.com - https://api.calix.ai/ - https://cloud-devfunc.calix.com/login - https://devfunc-rgw.calix.com - https://cloud-stg.calix.com/login - https://calixcloud-ca.calix.com/login - https://stage.api.calix.ai/ - https://rgw.calix.ai - https://calixcloud.calix.com/login	com/codelightband/smarthome/main/C alixUigaspiveApplication.java
https://another.com	com/canx/peopleui/peoplecompose/W ebsitesUiKt.java
https://www.calix.com/pages/pp/commandiq-privacy-policy.html	com/calix/settingsui/settings/SettingPr ivacyPolicyUiKt.java
2.5.29.35	sdk/pendo/io/k/i.java
2.5.29.15 2.5.29.19	com/koushikdutta/async/AsyncSSLSock etWrapper.java
https://ktor.io/docs/faq.html#no-transformation-found-exception	io/ktor/client/call/NoTransformationFo undException.java

2.5.4.10 2.5.4.13 2.5.4.5 2.5.4.9 2.5.4.6 2.5.4.43 2.5.4.7 2.5.4.72 2.5.4.44 2.5.4.8 2.5.4.3 2.5.4.17 2.5.4.4 2.5.4.65 2.5.4.15 2.5.4.11 2.5.4.42 2.5.4.54 2.5.4.12 2.5.4.45 2.5.4.16 2.5.4.46	sdk/pendo/io/d4/b.java
3.1.2.1	sdk/pendo/io/s3/a.java
https://play.google.com/store/apps/details?id=com.arlo.app&hl=en_in&gl=us	com/calix/networkui/activities/ArloListActivity.java
- https://stage.rgw.calix.ai - https://dev.rgw.calix.ai - https://rgw.ca.calix.com - https://devfunc-rgw.calix.com - https://rgw.calix.ai	com/cdelightband/smarthome/utils/PreferenceUtil.java
- http://www.speedtest.net/ - http://www.speedtest.net/privacy	com/cdelightband/smarthome/v5/V5BandwidthTest.java
- https://itunes.apple.com/cr/app/crbot/id1048473097?l=en&mt=8 - https://cdelightband.com/privacy-policy/ - https://stage.rgw.calix.ai/ - https://play.google.com/store/apps/details?id=net.crdroid	自研引擎-S

 Firebase 配置安全检测

标题	严重程度	描述信息
Firebase远程配置已禁用	安全	Firebase远程配置URL（https://firebase-remoteconfig.googleapis.com/v1/projects/422938982286/namespace/firebase:fetch?key=AIzaSyCpr1zKoMoW-uXjcr2WfXRBBGXeMjrd-LM）已禁用。响应内容如下所示： <pre>{ "state": "NO_TEMPLATE" }</pre>

第三方 SDK 组件分析

SDK名称	开发者	描述信息
Jetpack Test	Google	在 Android 中进行测试。
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。
Dexter	Karumi	Dexter 是一个 Android 库，它简化了运行时请求权限的过程。
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。
Jetpack ProfileInstaller	Google	让库能够提前预填充来自 ART 读取的编译轨迹。
Firebase Analytics	Google	Google Analytics (分析) 是一款免费的应用衡量解决方案，可提供关于应用使用情况和用户互动度的分析数据。
Jetpack AppCompat	Google	Allows access to new APIs on older API versions of the platform (many using Material Design).

邮箱地址敏感信息提取

EMAIL	源码文件
this@copy.slice	io/ktor/util/NIOkt.java
ggg@gmail.com	com/calix/uitoolkit/compose/basic/PopupEmailInputTextKt.java
tanya@calix.com	com/calix/uitoolkit/compose/basic/settings/ContactSupportTextKt.java
lsdksa@klsadk.ck	com/calix/uitoolkit/compose/basic/mynetwork/NetworkEditTextPasswordKt.java
lsdggggksa@klsadk.ck	com/calix/uitoolkit/compose/basic/EmailInputFieldKt.java
lsdksa@klsadk.ck	com/calix/uitoolkit/compose/basic/NewEmailInputFieldKt.java
lsdksa@klsadk.ck	com/calix/uitoolkit/compose/basic/PasswordInputFieldKt.java

第三方追踪器检测

名称	类别	网址
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Pendo	Analytics	https://reports.exodus-privacy.eu.org/trackers/416

🔑 敏感凭证泄露检测

可能的密钥
凭证信息=> "io.fabric.ApiKey" : "3ff853f40dcf4825bbda707c2f587744b4ad7801"
"android_key_store" : "AndroidKeyStore"
"com.google.firebase.crashlytics.mapping_file_id" : "00000000000000000000000000000000"
"google_api_key" : "AIzaSyCpr1zKoMoW-uXjcr2WfXRBbGXeMjrd-LM"
"google_app_id" : "1:422938982286:android:56b9ab8b23a5b685dc56df"
"google_crash_reporting_api_key" : "AIzaSyCpr1zKoMoW-uXjcr2WfXRBbGXeMjrd-LM"
"login_pwd_edit" : "com.calix.smarthome:id/login_pwd_edt"
"login_pwd_icon" : "com.calix.smarthome:id/pwd_in_visible_img"
"network_pwd_icon" : "com.calix.smarthome:id/pwd_in_visible_img"
"password" : "Password"
"password_txt" : "com.calix.smarthome:id/password_txt"
"pnd_app_id_testing" : "pnd_app_id_testing"
"pwd" : "Password"
"pwd_edt" : "com.calix.smarthome:id/pwd_edt"
"pwd_in_visible_img" : "com.calix.smarthome:id/pwd_in_visible_img"
"pwd_show_img" : "com.calix.smarthome:id/pwd_show_img"
"reg_pwd_edt" : "com.calix.smarthome:id/reg_pwd_edt"
"android_key_store" : "AndroidKeyStore"
"pwd" : "Kennwort"
"wifi_pas" : "WLAN-Kennwort"
"wifi_pwd" : "WLAN-Kennwort"
"android_key_store" : "AndroidKeyStore"

"android_key_store" : "AndroidKeyStore"
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE65381FFFFFFFFFFFFFFFF
32670510020758816978083085130507043184471273380659243275938904335757337482424
678471b27a9cf44ee91a49c5147db1a9aaf244f05a434d6486931d2d14271b9e35030b71fd73da179069b32e2935630e1c2062354d0da20a6c416e50be794ca4
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311591440858037121987999716643812574028291115057151
27580193559959705877849011840389048093056905856361568521428707301988689241309860865136260764883745107765439761230575
MIGfMA0GCSqGSIB3DQEBAQUAA4GNADCBiQKBgQCv8IqRRwpH8s7EnWhLwuFqnbTA
u2lkAvmqraDSBoHNeFDOS3fduZoc
O2ZzFxuj7V7FpPGrNdeLHdJ5y2Hrk9AN
Ct4eTIXHBIY2EaV7t7LjJaynVJCpkv4LKjTTAumiGUIuQhrNhZLuF
9DEF3CAFB939277AB1F12A8617A47BBDBA51DF499AC4C80BEEEA9614B19CC4D574F5E356E27CBDE51C6794BE24607A291558903BA0D0F84380B655BB9A22E8DCDF028A7CEC67F0D08134B1C8B97989149B609E0BE3BAB63D475783710DBC5B1FC764E3F4B53D09DA1158BFD3E2B9C8CF56EDF019539349627DB2FD53D24B7C48665772E437D6C7F8CE442734AF7CCB7AE837C264AF6A9BEB87F8A2FE5B8E5292E5A021FFF5E91479E8CE7A28C2442C6F315180F93499A234DCF76E3FED135F9BB
nMcadFr9rxwGUMGOn8qIcjLE4vr9T1rxm6DekW9IBGNAwGOv4UA7epTfpfPMYY8nO
b0b4417601b59cbc9d8ac8f935cadaec4f5fbb2f23785609ae4b6748d9b5a536
fca682ce8e12caba26efccf7110e526db078b05ede6b41eb4a208f3ae1617aeb01f5b07a47e6df63413c5e12ed0899bcd132acd50d99151bdc43ee737592e17
41058363725152142129326129780047268409c14441015993725554b35256314039467401291
MIGfMA0GCSqGSIB3DQEBAQUAA4GNADCBiQKBgQCbelsidvdpLGmRF3pex4Ar1HNI
m1735SettingPasscodeUAnknjM

FFFFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3DF1ED5D5FD65612433F51F5F066ED085636553DDED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB182B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9CE98583FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFFA886B4238611FCFDCDE355B3B6519035BBC34F4DEF99C023861B46FC9D6E6C9077AD91D2691F7F7EE598CB0FAC186D91CAEFE130985139270B4130C93BC437944F4FD4452E2D74DD364F2E21E71F54BFF5CAE82AB9C9DF69EE86D2BC522363A0DABC521979B0DEADA1DBF9A42D5C4484E0ABCD06BFA53DDEF3C1B20EE3FD59D7C25E41D2B669E1EF16E6F52C3164DF4FB7930E9E4E58857B6AC7D5F42D69F6D187763CF1D5503400487F55BA57E31CC7A7135C886EFB4318AED6A1E012D9E6832A907600A918130C46DC778F971AD0038092999A333CB8B7A1A1DB93D7140003C2A4ECEA9F98D0ACCOA8291CDCEC97DCF8EC9B55A7F88A46B4DB5A851F44182E1C68A007E5E0DD9020BFD64B645036C7A4E677D2C38532A3A23BA4442CAF53EA63BB454329B7624C8917BDD64B1C0FD4CB38E8C334C701C3ACDAD0657FCCFEC719B1F5C3E4E46041F388147FB4CFDB477A52471F7A9A96910B855322EDB6340D8A00EF092350511E30ABEC1FFF9E3A26E7FB29F8C183023C3587E38DA0077D9B4763E4E4B94B2BBC194C6651E776AF992EEAAC0232A281BF6B3A739C1226116820AE8DB5847A67CBEF9C9091B462D538CD72B03746AE77F5E62292C311562A846505DC82DB854433AE4915235C95B91178CCF2DD5CACEF403EC9D1810C6272B045B3B71F9DC6B80D63FDD4A8E9ADB1E6962A69526D43161C1A41D570D7938DAD4A40E329CCFF46AA36AD004CF600C8381E425A31D951AE64FDB23FCCE9509D43687FEB69EDD1CC5E0B8CC3BDF64B10EF86B63142A3AB832935B2F747C932665CB2C0F1CC01BD70229388839D2AF05E454504AC78B7582822846C0BA35C35F5C59160CC046FD8251541FC68C9C86B022BB7099876A460E7451A8A93109703FEE1C217E6C3826E52C51AA691E0E423CFC99E9E31650C1217B624816CDAD9A95F9D5B8019488D9C0A0A1FE3D75A517E23183F81D4A3F2FA4571EFC8CE0BA8A4FE8B6855DFE72B0A66EDED2FBABFBE58A30FAFABE1C5D71A87E2F741EF8C1FE86FEA6BBBF0E530C7770D97D11D49F7A8443D0822E506A9F4614E011E2A94838FF88CD68C8BB7C5C6424CFFFFFFFFFFF
FFFFFFFFFFFFFF90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A63A3620FFFFFFFFFFFFFF
m2054ShareNetworkQrDialogpzZJ40c
e9e642599d355f37c97ffd3567120b8e25c9cd43e927b3a9670fbec5d890141922d2c3b3ad2430093799869d1e84faab49fab0ad26d2ce6a22219d470bce7d777d4a21f1be9c270b57f607002f3cef8393694cf45ee3688c11a8c56ab127a3daf
m2206SectionBreakTitleWithCancelDIANMbU
f7e1a085d69b3ddecbcbab5c36b857b97994afbbfa3aea82f9574c0b7d0782675159578ebad4594fe67107108180b449167123e84c281613b7cf09328cc8a6e13c167a8b547c8d28e0a3ae1e2bb3a675916ea37f0bfa2135617fb027a01243bcc4f1bea8519089a883dfe15ae59f06928b665e807b552564014c3bfecf492a
36134250956749795798585127919587881956611103677985015071877198253563414405109
77d0f8c4dad15eb8c4f2f8d6726cefd96d5bb599
8d5155894229d5e689ee01e6018a231e2cae64cd
VTdL1VbC2tejvcI2BIMkEpk1BxPZ10KQ30GaDWFLN
FFFFFFFFFFFFFF90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A63A3620FFFFFFFFFFFFFF
2f19adeb284eb36f7f07786152c9a1d14b21653203ad0b04ebbf9c73ab6d7625
726838724295608800549323807888004534353641360687318060281490199180612328166730772686396383698676545930088884461843637361053498018365439
39402000036594479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112316

FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F45C2C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64ECFB850458DBEF0A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D2261AD2EE6BF12FFA06D98A0864D87602733EC86A64521F2B18177B200CBBE117577A615D6C770988C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A92108011A723C12A787E6D788719A10BDBA5B2699C327186AF4E23C1A946834B6150BDA2583E9CA2AD44CE8DBBBCC2DB04DE8EF92E8EFC141FBECBA6287C59474E6BC05D99B2964FA090C3A2233BA186515BE7ED1F612970CEE2D7AFB81BDD762170481CD0069127D5B05AA993B4EA988D8FDDC186FFB7DC90A6C08F4DF435C93402849236C3FAB4D27C7026C1D4DCB2602646DEC9751E763DBA37BDF8FF9406AD9E530EE5DB382F413001AEB06A53ED9027D831179727B0865A8918DA3EDBEBCF9B14ED44CE6CBACED4BB1BDB7F1447E6CC254B332051512BD7AF426FB8F401378CD2BF5983CA01C64B92ECF032EA15D1721D03F482D7CE6E74FEF6D55E702F46980C82B5A84C31900B1C9E59E7C97FBEC7E8F323A97A7E36CC88BE0F1D45B7FF585AC54BD407B22B4154AACCF86D7EBF48E1D814CC5ED20F8037E0A79715EEF798E32806A1D58BB7C5DA76F550AA3D8A1FBFF0EB19CCB1A313D55CDA56C9EC2EF29632387FE8D76E3C0468043E8F663F4860EE12BF2D5B0B7474D5E694F91E6DBE115974A3926F12FEE5E438777CB6A932DF8CD8BEC4D073B931BA3BC832B68D9DD300741FA7BF8AFC47ED2576F6936BA4246F3AAB3639C5AE4F5683423B4742BF1C978238F16CBE39D652DE3FDB8BEFC848AD92222E04A4037C0713EB57A81A23F0C73473FC646CEA306B4BCBC862F8385DDFA9D4B7FA2C087E879683303ED5BDD3A062B3CF5B3A278A66D2A13F83F44F82DDF310EE074AB6A364597E899A0255DC164FB31CC50846851DF9AB48195DED7EA1B1D510BD7EE74D73FAF36BC31ECFA268359046F4EB879F924009438B481C6CD7889A002ED5EE382BC9190DA61C626E479558E4475677E9AA9E3050E2765694DFC81F56E880B96E7160C980DD98EDD3DFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3DF1ED5D5FD65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB182B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9CE98583FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFA886B4238611FCFDCDE355B3B6519035BBC34F4DEF99C023861B46FC916F6C9077AD91D2691F7F71EF99CB0FAC186D91CAEFE130985139270B4130C93BC437944F4FD4452E2D74DD364F2E21E71F54BFF5CAE82AB9C9DF9E286D2BC522363A0DABC521979B0DEADA1DBF9A42D5C4484E0ABCD06BFA53DDEF3C1B20EE3FD59D7C25E41D2B669E1EF16E6F52C3164BF4FB7930E9E4E58857B6AC7D5742D89F6D187763CF1D5503400487F55BA57E31CC7A7135C886EFB4318AED6A1E012D9E6832A907600A918130C46D173F971AD0038092999A333CB8B7A1A1DB93D7140003C2A4ECEA9F98D0ACCOA8291CDCEC97DCF8EC9B55A7F88A46B4DB5A851F44182E1C87A007F5E0DD9020BFD648646036C7A4E677D2C38532A3A23BA4442CAF53EA63BB454329B7624C8917BDD64B1C0FD4CB38E8C334C701C3ACDAD0657F2CFEC719B1F5C3E4146041F388147FB4CFDB477A52471F7A9A96910B855322EDB6340D8A00EF092350511E30ABEC1FFF9E3A26E7FB29F8C183C23C3587E38DA0077D954763E4E4B94B2BBC194C6651E77CAF992EEAAC0232A281BF6B3A739C1226116820AE8DB5847A67CBEF9C9091B467D5181D72B03746AE77F5E3292C311562A846505DC82DB854338AE49F5235C95B91178CCF2DD5CACF403EC9D1810C6272B045B3B71F9DC6B80D635DD4A8E9ADB1E6962A69525D43161C1A41D570D7938DAD4A40E329CD0E40E65FFFFFFFFFFFFFFFFF
115792089237316195423570985008687907853269984665640564039457584007408831671663
39402006196394479212279040100143613805079739270465446667946905279621659399113263569398956308152294913554433653942643
57896044618658097711785492504343957926634992332820282019728792003956564819949
11579208923731619542357098500868790785283756427907494292605163141518161494337
9cdbd84c9f1ac2f38d1f8b142ab952e7338bf511
962eddcc369c9a8c9b1260ee6b6a126d9346e38b6
FDB497F16F9D71A89D042B0FA5B7741E45EE7938F08CFDA9F1FB58EBDF749E7
32b69d30fbd741b08dc834d6c269041e
8138e8a0fcf3a4e84a711149fd305d7f4aa59306d7251de54d98af8fe95729a1f73d893fa424cd2edc8636a6c3285e022b0e3866a565ae8108eed8591cd4fe8d2ce86165a978d715eb1647f362d33fca29cd179fb42401cbaf3df0c614056f9c8f3cfd51e474afb6bc6974f78db8aba8e9e517fded658591ab7502bd41849462f
FFFFFFFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3DF1ED5D5FD65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB182B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9CE98583FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFA886B423861285C97FFFFFFFFFFFFFFFFF

FFFFFFFF90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8ACAA68FFFFFFFFFFFFF
EEAF0AB9ADB38DD69C33F80AFA8FC5E86072618775FF3C0B9EA2314C9C256576D674DF7496EA81D3383B4813D692C6E0E0D5D8E250B98BE48E495C1D6089DAD15DC7D7B46154D6B6CE8EF4AD69B15D4982559B297BCF1885C529F56660E57EC68EDBC3C05726CC02FD4CBF4976EAA9AFD5138FE8376435B9FC61D2FC0EB06E3
ptBOOQfVh6dD741ykvxHjgupulJlnHGa
AC6BDB41324A9ABF166DE5E1389582FAF72B6651987EE07FC3192943DB56050A37329CBB4A099ED8193E0757767A13DD52312AB1B03310DCD7F48A9DA04FD50E8083969EDB767B0CF6095179A163AB3661A05FBD5FAAAE82918A9962F0B93B855F97993EC975EEAA80D740ADB74FF747359D041D5C33EA71D281E446B14773BCA97B43A23FB801676BD207A436C6481F1D2B9078717461A5B9D32E688F87748544523B574B0D57D5EA77A2775D2ECFA032CFBDBF52FB3786160279004E57AE6AF874E7303CE53299CC041C7BC308D82A5698F3A8D0C38271AE35F8E9D7FBB694B5C803D89F7AE435DE236D525F54759B65E372FCD68EF20FA7111F9E4AFF73
m1052ArloListOfCameraServiceUiDIANMbU
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122555640661454554977296311391480858037121987999716643812574028291115057148
MIGfMA0GCSqGSIlb3DQEBAQUAA4GNADCBiQKBgQC1B6qsa2sbpc4CuFEjgRWez9nV
m1726SecondaryAdminDetailsUiZPw9REg
115792089210356248762697446949407573530086143415290314195533631308867097853948
109384903807373427451111239076680556993620759895168374899438694495953116150735016013708737573759623248592132296706313309438452531591012912142327488478985984
115792089210356248762697446949407573530086143415290314195533631308867097853951
f8183668ba5fc5bb06b5981e6d8b795d30b8978d43cd0cc572e37e09939a9773
42debb9da5b3d88cc956e08787ec3fa09bbba5f43bb889a74aaf5317aa0fbb7e3c5b8fcd7a53bef563b0e98560328960a9517f4014d3325fc7962bf1e049370d76d1314a76137e792f3f0db8596095ea5b932024f079ecf25f0f0297452b0770e1350782ed57ddf794979dcef23cb96f183061965c4ebc93c9c71c56b925955a75f94cccf1449ac43d586dd0b6ee43251b0b2287349d68dfe9d444403f13e802f4146d882e057af19b6f6275c6676c8fa0e3ca2713a3257fd1b27d0639f695e347d8d1cf9ac819a56ca9b04cb0eb9b7b035988d15bbac65212a55239cfc7e58fae38d7250ab9991ffbc97134025fe8ce04c4399ad96569be91a546f4978693c7a
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340371808892707005449
7cac391922981b6184bdce1fd9834c259181f5abf91ded6078210d0f91ace360
b869c82b35d70e1b1ff91b28e37a62ecdc34409b
258EAFa5-E914-47DA-93C4-C5A80DC85B11
2624703509579568268623156744566981891852923491109213387815615900925518854738050089022388053975719786650872476732087
m2257SecondaryAdminProfileViewZPw9REg
kK1cj0mRj7iSmTft3vAGO44vobsu36op
48439561293906451759052585252797914202762949526041747995844080717082404635286

30470ad5a005fb14ce2d9dcd87e38bc7d1b1c5facbaecbe95f190aa7a31d23c4dbbcbe06174544401a5b2c020965d8c2bd2171d3668445771f74ba084d2029d83c1c158547f3a9f1a2715be23d51ae4d3e5a1f6a7064f316933a346d3f529252
fd7f53811d75122952df4a9c2eece4e7f611b7523cef4400c31e3f80b6512669455d402251fb593d8d58fabfc5f5ba30f6cb9b556cd7813b801d346ff26660b76b9950a5a49f9fe8047b1022c24fbba9d7feb7c61bf83b57e7c6a8a6150f04fb83fd6d3c51ec3023554135a169132f675f3ae2b61d72aeff22203199dd14801c7
FFFFFFFFFFFFFFFFFADF85458A2BB4A9AAFD5C5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE362630C75D8F681B202AEC4617AD3DF1ED5D5FD65612433F51F5F066ED085636553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB182B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9CE98583FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFAA886B4238611FCFDCDE355B3B6519035BBC34F4DEF99C023861B46FC9D6E6C9077AD91D2691F7F7EE598CB0FAC186D91CAEFE130985139270B4130C93BC437944F4FD4452E2D74DD364F2E21E71F54BFF5CAE82AB9C9DF69EE86D2BC522363A0DABC521979B0DEADA1DBF9A42D5C4484E0ABCD06BFA53DDEF3C1B20EE3FD59D7C25E41D2B66C62E37FFFFFFFFFFFFFFFF
eyJkYXRhY2VudG9yJjoidXMlLCJrZXkiOiJjZiNGVmYyU1Nzc0OWNmZmNmYmRmODkxNmZiZTgwZTdlYjRmYyY3YjA5MjQ3MGUwNWY2ZTVkNjgyY2U0OWNiZTg3NWxMGM3YzE2YzZhMWYmYzNiZDkwMGYxOWU2ZTFmMGUzNzBiMTBmN2E4NDQ1NDUgZjQ5MWQxODQ1ZjI1MTIzZDhkNTg2YWNhYmZhY2Y0OWFjODU2YjA4Njg5ODQzLjlkZmY0OGUwMTJhYWVlNDhNDA3NW1NDk0ODEzNzY1NDY1MjIjLjE3OTM1MmNkNWl5MTQwNTIwNjRhM2ZlMzZlNTMwMWI0OTcwNzBhMTdlOTMxNGQzNDg1ODIifQ
9760508f15230bccb292b982a2eb840bf0581cf5
f1e8f309a51fd2ce04ba280552a9241f37fadab4d9da7c729ec9630a588e4c10
55066263022277343669578718895168534326250603453777594175500187960889116729240
FFFFFFFFFFFFFFFFFADF85458A2BB4A9AAFD5C5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE362630C75D8F681B202AEC4617AD3DF1ED5D5FD65612433F51F5F066ED085636553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB182B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9CE98583FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFAA886B4238611FCFDCDE355B3B6519035BBC34F4DEF99C023861B46FC9D6E6C9077AD91D2691F7F7EE598CB0FAC186D91CAEFE130985139270B4130C93BC437944F4FD4452E2D74DD364F2E21E71F54BFF5CAE82AB9C9DF69EE86D2BC522363A0DABC521979B0DEADA1DBF9A42D5C4484E0ABCD06BFA53DDEF3C1B20EE3FD59D7C25E41D2B66C62E37FFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFF90FDAA22168C234C4C6628B80DC1CD129024A088AA67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA23361C55D39A69163FA8FD24C5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C3290BE462E20CE3BE39E772C120E85039E72783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AAAC42ADAD33170D04507A3378521ABDF1CBA64ECF8B850458DBEF0A8EA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04125613DCCEE3D2261AD2E76B512FA06D98A0864D87602733CE86A64521F2B18177B200CBBE117577A615D6C770988C0BAD946E208E24FA074E5A6512DB5BFCE0FD108E4B2D120A92108011A723C12A787E6D788719A10BDBA5B2699C327186AF4E23C1A946834B6150BDA2583E9CA2AD44CE8DBBBBC2DB04DE8EF92E8FCA41FBECAA6287C59474E6BC05D99B2964FA090C3A2233BA186515BE7ED1F612970CEE2D7AFB81BDD7621704871D0009127D5B05AA993B4FA93BD3FDCC186FFB7DC90A6C08F4DF435C93402849236C3FAB4D27C7026C1D4DCB2602646DEC9751E763DBA37BDF8F79406AD9E530EE5D3B82F413001AEB06A53ED9027D831179727B0865A8918DA3EDBEBCF9B14ED44CE6CBACED4BB1BDB7F1447E6CC254B332051512BD7AF426FB8F401378CQ2BF5983CA01C64B92ECF032EA15D1721D03F482D7CE6E74FEF6D55E702F46980C82B5A84031900B1C9E59E7C97FBEC7E8F323A97A7E36CC8B20F1D45B7FF585AC54BD407B22B4154AAC8F6D7EBF48E1D814CC5ED20F8037E0A79715EEF29BE32806A1D58B7B7C5DA76F550AA3D8A7F5BF50EB19CCB1A313D55CDA56C9EC2EF29632387FE8D76E3C0468043E8F663F4860EE12BF2D5B0B7474D6E694F91E6DCC4024FFFFFFFFFFFFEFFF
95475cf5d93e59f6c3fcd1d902add02f427f5f3c7210313bb45fb4d5bb2e5fe1cbd678cd4bbdd84c9836be1f31c077725aeb6c2fc38b85f48076fa76bcd8146cc89a7b2f706dd719898c2083dc8d896f84062e2c9c94d137b054a8d8096adb8d51952398eeca852a0af12df83e475aa65d4ec0c38a9560d5661186ff98b9fc9e96eeeb030376b236bc73be3acdbd74fd61c1d2475fa3077b8f080467881ff7e1ca56fee066d79506ade51edbb5443a563927dbc4ba520086746175c8885925ebc64c6147906773496990cb714ec667304e261faee33b3cbd0f008e0c3fa90650d97d3909c9275bf4ac86ffcb3d03e6dfc8ada5934242dd6d3bccaa2a406cb0b

FFFFFFFF90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA237327FFFFFFFFFFFFFFF
Vd99BKhp3mXSDJzHuVrCq52xBXAKVahbuFb6dqBc
FFFFFFFF90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CFA916AE515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64ECFB850458DBEF0A8AEA71575D060C7DB3970F85A6E1F4C7ABF5AE8CDB0933D71E8C94E04A25619DC EE3D2261AD2EE6BF12FFA06D98A0864D87602733EC86A64521F2B18177B200CBBE117577A015D6C770988C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A92108011A723C12A787E6D788719A10BDBA5B2699C327186AF4E2311A46534B6150BDA2583E9CA2AD44CE8DBBCC2DB04DE8EF92E8EFC141FBEC A6287C59474E6BC05D99B2964FA090C3A2233BA186515BE7E11F612970CEE2D7AFB81BDD762170481CD0069127D5B05AA993B4EA988D8FDDC186FFB7DC90A6C08F4DF435C934063199FFFFFFFFFFFFFFF
266174080205021706322876871672336096072985916875697314770667136841880294499642780849154508962771902352094241225065558662157113545570916814161637315895999846
37571800257700204635455072244911836035944551347697624866945677796155444774405563166912344050129455395621444457289428522585666729196580810124344277578376784
39402006196394479212279040100143613805079739270465446667948293404245721771406870329047266088258938001861606973112319
115792089210356248762697446949407573529996955224135760342422259061068512044369
m2064SharedNetworkQrDialogButton8V94
nvknbo5+6pBVWVZpCg5RtpiijUKMxOmJrccBCo7ICiQPIj/L9Nc5zmWlH2igKHLq
aOmB8NSUjxGRUMmQeSZz1hD9BZZMb5wkM8POIIDEgfnadTbXEx1ZQbmcATG2sup2G7x4Bzvb74KpZHeHp7FRCUmIYBZNH1Z
sXchDaQebHnPiGvyDOAT4saGEUetSyo9MKLOpWf-guEr23bOdgWp4Dy1WUteWbqBHod5pcM9H95GQRV3JDXboiRROSBigcC5yjU1hGzHHyXss8UDprecbaYxknTcQkhsiANGRUZmdTOQ5gnTsLaf63YuyvVRdhS8exS3Ej

► Google Play 应用市场信息

标题: CDE Smartband

评分: 4.8333335 安装: 1,000+ 价格: 0 **Android**版本支持: 分类: 办公 **Play Store URL:** <com.cdelightband.smarthome>

开发者信息: Clarksville Department of Electricity, Clarksville+Department+of+Electricity, None, None, CustomerService@cdelightband.com,

发布日期: 2022年9月7日 隐私政策: [Privacy link](#)

关于此应用

CDE Lightband 允许用户保护和他们的家庭 Wi-Fi 网络。使用网络安全、SSID 和密码管理等应用程序功能保护您的家。使用家长控制等应用程序功能进行控制，并阻止不需要的内容进入您的家。

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