南明离火
移动应用检测平台

ANDROID 静态分析报告

Ultra-SDP • v1.0.0

分析日期: 2024-03-14 13:37:53

应用概览

文件名称:	app-release.apk
文件大小:	24.2MB
应用名称:	Ultra-SDP
软件包名:	com.zta.android
主活动:	com.zta.android.news.activity.SplashActivity
版本号:	1.0.0
最小SDK:	20
目标SDK:	29
加固信息:	未加壳
应用程序安全分数:	48/100 (中风险)
杀软检测:	AI评估：很危险，请谨慎安装
MD5:	5418115cd4b552c4cd79d6d68815af17
SHA1:	da7eb5f8061f06e88399bdfac3959fa15546b45d
SHA256:	cc1bd39d601e3e82c670c569b295fbb47cb40e1947866b7849c4af86d44d3f

分析结果严重性分布

高危	中危	信息	安全	关注
5	8	2	3	9

四大组件导出状态统计

Activity组件：30个，其中export的有：2个
Service组件：2个，其中export的有：2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

本报告由南明离火移动安全分析平台生成

v3 签名: False
v4 签名: False
主题: C=cn, ST=beijing, L=beijing, O=zta, OU=zta, CN=zta
签名算法: rsassa_pkcs1v15
有效期自: 2021-11-08 08:34:19+00:00
有效期至: 2046-11-02 08:34:19+00:00
发行人: C=cn, ST=beijing, L=beijing, O=zta, OU=zta, CN=zta
序列号: 0x4986ce02
哈希算法: sha256
证书MD5: 62636d81a7d0828c1f740a7923b5d030
证书SHA1: 24ef25a1d0f107d104bcccf70e33cc25f0b4aa72
证书SHA256: b58b12d24087ac9fafd84a21c1a8002dc3e06df24240bf57c79b767975382e39
证书SHA512:
8bb2c26a08f324334fc8e27d7bc07f056c7bb11c20267e2d4ed25c575450ee1129a0949d8a5a529f12b696281c60f5dd13b6ff5e7e58f70d8fff9538e2d5e7fb

公钥算法: rsa
密钥长度: 2048
指纹: be4a2c129b0573fe309bbabd2b63f466cf073985cdeeed693cbf09b30fcf5974
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.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.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.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.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.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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
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.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.CHANGE_NETWORK_STATE	危险	改变网络连通性	允许应用程序改变网络连通性。
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.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.GET_TASKS	危险	检索当前运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。恶意应用程序可借此发现有关其他应用程序的保密信息。
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。

android.permission.REQUEST_INSTALL_PACKAGES	危险	允许安装应用程序	Android8.0 以上系统允许安装未知来源应用程序权限。
android.permission.CALL_PHONE	危险	直接拨打电话	允许应用程序直接拨打电话。恶意程序会在用户未知的情况下拨打电话造成损失。但不被允许拨打紧急电话。
android.permission.ACCESS_FINE_LOCATION	危险	获取精确位置	通过GPS芯片接收卫星的定位信息，定位精度达10米以内。恶意程序可以用它来确定您所在的位置。
android.permission.ACCESS_COARSE_LOCATION	危险	获取粗略位置	通过WiFi或移动基站的方式获取用户错略的经纬度信息，定位精度大概误差在30~1500米。恶意程序可以用它来确定您的大概位置。
android.permission.WAKE_LOCK	危险	防止手机休眠	允许应用程序防止手机休眠，在手机屏幕关闭后台进程仍然运行。
android.permission.DEVICE_POWER	签名	开机或关机	允许应用程序启动/关闭设备。
android.permission-group.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.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。
android.permission.KILL_BACKGROUND_PROCESSES	普通	结束进程	允许应用程序结束其他应用程序的后台进程。

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: **7** | 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 4.4W-4.4W.2, [minSdk=20]	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	应用程序具有网络安全配置 [android:networkSecurityConfig=@xml/network_security_config]	信息	网络安全配置功能让应用程序可以在一个安全的，声明式的配置文件中自定义他们的网络安全设置，而不需要修改应用程序代码。这些设置可以针对特定的域名和特定的应用程序进行配置。
4	Activity (com.zta.android.activity.MainActivity) 未被保护。 存在一个intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。
5	Broadcast Receiver (com.zta.android.BootShutdownReceiver) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Broadcast Receiver是显式导出的。
6	Service (com.zta.android.backend.GoBackend$VpnService) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.BIND_VPN_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	Service (com.zta.android.QuickTileService) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.BIND_QUICK_SETTINGS_TILE [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。
8	Activity (com.zta.android.activity.ZtaMainActivity) 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。
9	Activity (com.zta.android.news.activity.HomeActivity) 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.xuexiang.xqrcode.ui.CaptureActivity) 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。

代码安全漏洞检测

高危: **2** | 警告: **9** | 信息: **2** | 安全: **2** | 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	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	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
5	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
6	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
7	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
8	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
9	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

本报告由南明离火移动安全分析平台生成

10	MD5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
11	此应用程序可能具有Root检测功能	安全	OWASP MASVS: MSTG-RESILIENCE-1	升级会员：解锁高级权限
12	此应用程序可能会请求root（超级用户）权限	警告	CWE: CWE-250: 以不必要的权限执行 OWASP MASVS: MSTG-RESILIENCE-1	升级会员：解锁高级权限
13	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
14	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
15	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

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)	SYMBOLS STRIPPED(裁剪符号表)

1	arm64-v8a/libztaapi.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: ['__memset_chk']	False warning 符号可用

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	11/30	android.permission.CAMERA android.permission.RECEIVE_BOOT_COMPLETED android.permission.RECORD_AUDIO android.permission.VIBRATE android.permission.GET_TASKS android.permission.READ_PHONE_STATE android.permission.REQUEST_INSTALL_PACKAGES android.permission.CALL_PHONE android.permission.ACCESS_FINE_LOCATION android.permission.ACCESS_COARSE_LOCATION android.permission.WAKE_LOCK
其它常用权限	8/46	android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.CHANGE_NETWORK_STATE android.permission.CHANGE_WIFI_STATE android.permission.FLASHLIGHT

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
xml.org	安全	否	**IP地址:** 104.239.240.11 **国家:** United States of America **地区:** Texas **城市:** Windcrest **纬度:** 29.499678 **经度:** -98.399246 **查看:** Google 地图

onekey1.cmpassport.com	安全	是	**IP地址:** 120.197.235.28 **国家:** China **地区:** Guangdong **城市:** Guangzhou **纬度:** 23.127361 **经度:** 113.264252 **查看:** 高德地图
log1.cmpassport.com	安全	是	**IP地址:** 36.138.255.61 **国家:** China **地区:** Gansu **城市:** Lanzhou **纬度:** 36.056389 **经度:** 103.792222 **查看:** 高德地图
config.cmpassport.com	安全	是	**IP地址:** 120.232.169.180 **国家:** China **地区:** Guangdong **城市:** Guangzhou **纬度:** 23.127361 **经度:** 113.264252 **查看:** 高德地图
www.cmpassport.com	安全	是	**IP地址:** 120.197.235.28 **国家:** China **地区:** Guangdong **城市:** Guangzhou **纬度:** 23.127361 **经度:** 113.264252 **查看:** 高德地图
user-gold-cdn.xitu.io	安全	否	No Geolocation information available.
ip.3322.net	安全	是	**IP地址:** 118.184.169.32 **国家:** China **地区:** Jiangsu **城市:** Changzhou **纬度:** 31.783331 **经度:** 119.966667 **查看:** 高德地图
download.wireguard.com	安全	否	**IP地址:** 136.144.57.121 **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
smsks1.cmpassport.com	安全	是	**IP地址:** 120.197.235.28 **国家:** China **地区:** Guangdong **城市:** Guangzhou **纬度:** 23.127361 **经度:** 113.264252 **查看:** 高德地图

juejin.im	安全	否	**IP地址:** 103.136.220.204 **国家:** Singapore **地区:** Singapore **城市:** Singapore **纬度:** 1.289670 **经度:** 103.850067 **查看:** Google 地图
photocdn.sohu.com	安全	是	**IP地址:** 180.97.228.140 **国家:** China **地区:** Jiangsu **城市:** Suzhou **纬度:** 31.311390 **经度:** 120.618051 **查看:** 高德地图
49d2147716ff75a9dc3c984f02381780.dd.cdntips.com	安全	是	**IP地址:** 27.232.162.21 **国家:** China **地区:** Hunan **城市:** Changsha **纬度:** 28.200001 **经度:** 112.966667 **查看:** 高德地图
p6-juejin.byteimg.com	安全	是	**IP地址:** 42.81.247.47 **国家:** China **地区:** Tianjin **城市:** Tianjin **纬度:** 39.142220 **经度:** 117.176666 **查看:** 高德地图

URL 链接安全分析

URL信息	源码文件
• 255.255.255.128 • 255.255.255.192 • 255.255.255.224 • 255.255.255.240 • 255.255.255.248 • 255.255.255.252 • 255.255.255.254 • 255.255.255.255	cn/hutool/core/net/MaskBit.java
• 10.255.255.255 • 172.31.255.255 • 192.168.255.255	cn/hutool/core/net/NetUtil.java
• http://xml.apache.org/xslt}indent-amount • http://apache.org/xml/features/disallow-doctype-decl • http://xml.org/sax/features/external-general-entities • http://xml.org/sax/features/external-parameter-entities • http://apache.org/xml/features/nonvalidating/load-external-dtd	cn/hutool/core/util/XmlUtil.java
• 2.5.29.15	cn/hutool/crypto/asymmetric/Sign.java
• data:image	com/bumptech/glide/load/model/DataUrlLoader.java

• 5.4.9.1	com/cmic/sso/sdk/auth/AuthnHelper.java
• http://www.cmpassport.com/unisdk/ • https://www.cmpassport.com/unisdk/rs/simQuickAuthReq • https://www.cmpassport.com/unisdk/rs/simQuickAuthCheck • https://smsks1.cmpassport.com/unisdk/ • https://onekey1.cmpassport.com/unisdk/rs/sendsms • https://onekey1.cmpassport.com/unisdk/ • https://config.cmpassport.com:443/client/uniConfig	com/cmic/sso/sdk/b/b/a.java
• https://log1.cmpassport.com:9443/log/logReport	com/cmic/sso/sdk/c/b.java
• https://smsks1.cmpassport.com/unisdk/ • https://onekey1.cmpassport.com/unisdk/ • https://log1.cmpassport.com:9443/log/logReport • http://www.cmpassport.com/unisdk/	com/cmic/sso/sdk/d/g.java
• 223.5.5.5	com/xuexiang/xutil/net/NetworkUtils.java
• http://192.168.1.103/ztaclient/index_app_new.html?token=eyJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJ0eGEiLCJpc3MiOiJodHRwOlwvXC93d3cuenRhLmNvbSIsImV4cCI6MTYwODcyODgyMCwidXNlcmlkIjoiMjMsTQxNmU0MTVmNGExZiJ9.VR8NjAvlVAJ2AQ7LI-yMJ9Rzqku7_V0bk2aL-b8qoA0	com/zta/android/activity/MainWebViewActivity.java
• http://www.baidu.com	com/zta/android/activity/ZtaMainActivity.java
• http://192.168.187.197:8080/SmartSdp	com/zta/android/news/fragment/AboutFragment.java
• https://49d2147716ff75a9dc3c984f02381780.dd.cdntips.com/	com/zta/android/news/update/RetrofitHelper.java
• http://photocdn.sohu.com/tvmobilemvms/20150902/144150323071011277.jpg • http://photocdn.sohu.com/tvmobilemvms/20150907/144158380433341332.jpg • http://photocdn.sohu.com/tvmobilemvms/20150907/144160286644953423.jpg • http://photocdn.sohu.com/tvmobilemvms/20150902/144115156939164801.jpg • http://photocdn.sohu.com/tvmobilemvms/20150907/144159406950245647.jpg • http://mp.weixin.qq.com/mp/homepage?__biz=Mzg2NjA3NDIyMA==&hid=5&sn=bdee5aafe9cc2e0a618d055117c84139&scene=18#wechat_redirect • https://p6-juejin.byteimg.com/tos-cn-i-k3u1fbpfcp/463930705a844f638433d1b26273a7cf~tplv-k3u1fbpfcp-watermark.image • https://juejin.im/post/5c2ed1dae51d4543805ea48d • https://user-gold-cdn.xitu.io/2019/1/16/1685563e14b6408?imageView2/0/w/1280/h/960/format/webp/ignore-error/1 • https://juejin.im/post/5b480b79e51d451909c5e144 • https://user-gold-cdn.xitu.io/2018/7/13/164d92d9b7877dc21?imageView2/0/w/1280/h/960/format/webp/ignore-error/1 • https://juejin.im/post/5b6b9b40e51d4576b828978d • https://user-gold-cdn.xitu.io/2018/8/9/1651c568a7e30e02?imageView2/0/w/1280/h/960/format/webp/ignore-error/1 • https://juejin.im/post/5c6fc0cdf265da2dda694f05 • https://user-gold-cdn.xitu.io/2019/2/22/16914891cd8a950a?imageView2/0/w/1280/h/960/format/webp/ignore-error/1	com/zta/android/news/util/DemoDataProvider.java
• https://www.baidu.com/	com/zta/android/preference/VersionPreference.java
• https://download.wireguard.com/android-module/modules.txt.sig • https://download.wireguard.com/android-module/%s	com/zta/android/util/ModuleLoader.java

本报告由南明离火移动安全分析平台生成

• https://ip.3322.net/	com/zta/util/DeviceTool.java

- data:image
- 10.255.255.255
- https://download.wireguard.com/android-module/modules.txt.sig
- 255.255.255.192
- 255.255.255.252
- 192.168.255.255
- http://apache.org/xml/features/nonvalidating/load-external-dtd
- https://smsks1.cmpassport.com/unisdk/
- https://download.wireguard.com/android-module/%s
- 172.31.255.255
- 5.4.9.1
- 255.255.255.254
- https://www.cmpassport.com/unisdk/rs/simQuickAuthCheck
- http://xml.org/sax/features/external-general-entities
- 255.255.255.240
- https://log1.cmpassport.com:9443/log/logReport
- http://xml.org/sax/features/external-parameter-entities
- https://www.cmpassport.com/unisdk/rs/simQuickAuthReq
- 255.255.255.128
- http://ns.adobe.com/xap/1.0/
- https://issuetracker.google.com/issues/116541301
- 255.255.255.224
- 2.5.29.15
- https://onekey1.cmpassport.com/unisdk/rs/sendsms
- https://onekey1.cmpassport.com/unisdk/
- http://xml.apache.org/xslt}indent-amount
- http://apache.org/xml/features/disallow-doctype-decl
- https://config.cmpassport.com:443/client/uniConfig
- 255.255.255.248
- 255.255.255.255
- http://www.cmpassport.com/unisdk/
- http://192.168.187.197:8080/SmartSdp

自研引擎分析结果

第三方 SDK 组件分析

SDK名称	开发者	描述信息
WireGuard	Jason A. Donenfeld	WireGuard® is an extremely simple yet fast and modern VPN that utilizes state-of-the-art cryptography. It aims to be faster, simpler, leaner, and more useful than IPsec, while avoiding the massive headache. It intends to be considerably more performant than OpenVPN. WireGuard is designed as a general purpose VPN for running on embedded interfaces and super computers alike, fit for many different circumstances. Initially released for the Linux kernel, it is now cross-platform (Windows, macOS, BSD, iOS, Android) and widely deployable. It is currently under heavy development, but already it might be regarded as the most secure, easiest to use, and simplest VPN solution in the industry.
AndPermission	yanzhenjie	Android 平台上的权限管理器。
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 Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代

邮箱地址敏感信息提取

EMAIL	源码文件
auth-agent@openssh.com	cn/hutool/extra/ssh/ChannelType.java
permission@gmail.com	com/yanzhenjie/permission/checker/CalendarWriteTest.java
auth-agent@openssh.com	自研引擎分析结果

敏感凭证泄露检测

可能的密钥
"gusturepass_auth" : "手势密码认证"
9778397bd19801ec9210c965cc820e
97bd097bd097c36b0b6fc9210c8dc2
eyJzdWIiOiJ6dGFjLCJpc3MiOiJodHRwOlwvXC93d3cuenRhLmNvbSIsImV4cCI6MTYwODcyODgyMCwidXNlcmlkIjoiM2JmOTQxNmU0MTVmNGExZiJ9
04fff201a[illegible]e3e204843835134e6f2e6[illegible]22d4521db3ad35daa8e1fe60a343fa6438bc162a5dc9ff33dfec5faf377e54747c42626e9664c1127bfc70d2e5033a
bdee5aafe9cc2e0a618d085117c84139
977837f0e37f149[illegible]082b0787b0721
b0a00e4a271be[illegible]478e42fad0618432fa7d7fb3d99004d2b0bdfc14f8024832b
7f0e397bc09[illegible]c36b0b6fc9210c8dc2
7f07e7f0e47f531b0723b0b6fb0721

7f0e397bd07f595b0b6fc920fb0722
7f0e27f0e47f531b0b0bb0b6fb0722
97bcf97c359801ec95f8c965cc920f
665f67f0e37f14898082b0723b02d5
7ec967f0e37f14998082b0787b0721
7f07e7f0e37f149b0723b0787b0721
7f0e397bd097c35b0b6fc9210c8dc2
7f0e37f0e366aa89801eb072297c35
5c6fc0cdf265da2dda694f05
7f0e37f5307f595b0b0bc920fb0722
97b6b7f0e47f531b0723b0b6fb0721
X2ZpgqrBuxwT8M0mv1G7No5ptPM
7f0e397bd07f595b0b0bc920fb0722
665f67f0e37f14898082b072297c35
7f07e7f0e47f149b0723b0787b0721
5b480b79e51d45190905ef44
7ec967f0e37f14998082b0723b06bd
97bd097bd07f595b0b6fc920fb0722
nAoGBAIC5wrkORKug3gw+BwIEk3AEddLY[illegible]+w[illegible]qK[illegible]ceaxmTYIxQdGobl[illegible]p[illegible]AY[illegible]qt[illegible]d
7f07e7f0e37f14998083b0787b0721
977837f0e37f149b0723b0787b0721
7f0e37f1487f595b0b0bb0b6fb0722
7f07e7f0e47f531b0723b0b6fb0722
nPN6Dzx[illegible]XVx7w[illegible]XoXG4rnjD8/qoI[illegible]S71CuafyhqGhqdsTMKKL7njWvn0KWbdL
9778397bd097c36c9210c9274c91aa
7f0e36665b66aa89801e9808297c35
463930705a844[illegible]633433d[illegible]b26273a7cf
97b6b97bd19801ec95f8c965cc920f
ne6AxVJJ6[illegible]XQRkLEhmVTogfJFmQKXYeAoqNoMHkxtwJCTOQ==
nYv+u4FlvGiJIlKsmLJweIbAqVNOCOmJzP6ycgpxR8qDUSwYBAkEA1USGJq/3CLE4

7f0e27f1487f595b0b0bb0b6fb0722
97bd07f5307f595b0b0bc920fb0722
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/YHP9utFGOhGk7Xf5L7jOgQz5
97b6b7f0e47f531b0723b0b6fb0722
977837f0e37f14998082b0787b06bd
nqDETE6BELpBYKHeS7j3t8PsCFddxI0vgzUMzCP4DDX1Rigv8cAM6yOo9utiGDxwQ
5b6b9b49e51d4576b828978d
977837f0e37f14898082b0723b02d5
97b6b97bd197c36c9210c9274c920e
7f0e26665b66a449801e9808297c35
7f0e36665b66a449801e9808297c35
7f0e37f0e37f14898082b072297c35
7ec967f0e37f14898082b0723b02d5
MIICXgIBAAKBgQCkzAyTd86uiPMkvwGPevdr77TnoCAfpuruO5c6XnbcbaMevG3r
97b6b97bd19801ec9210c965cc920e
noLgqmma+jHAVyT5VzouzKIJNXy+WqahMN3vmLIt7ois7Vpt6131 WVNUN7+
9778397bd19801ec9210c9274c920e
9778397bd097c36b0b6fc9274c91aa
97b6b97bd19801ec9210c9274c920e
5a77595aec52733a5f54cf078821d2 e379550ac0654c178 1c50
a3785913ca4deb75abd84141 e879777940c78c bee6c0352
977837f0e37f14998082b0723b06bd
97b6b7f0e47f531b0723b0787b0721
nBl6croB FbAnIU8Nf95bHm1MW iN4yOgI+ig9qa4/IFFgH1RjQIDAQAB
b027097bd097c36b0b6fc9274c91aa
nq6s7XEjpZC4iyQhwZ 7QY+UJg67ECQQCDPKS03+nLnorWPu2aahOBeEfr
ngZlTTem7Pjdm QvFHsvT+vNgJ3wAIRd+iCMXm8y96yZhD2+SH5odBYS2
nY7XhFbhmf5B4+ PsjBNfUWNFHaMGOQJsQlz/lynGNpiEjnLHIfHh7foegdV9AkEA
7f0e397bd097c35b0b6fc920fb0722
7f0e27f1487f531b0b0bb0b6fb0722

665f67f0e37f1489801eb072297c35
97bcf7f1487f531b0b0bb0b6fb0722
7ec967f0e37f14998082b0787b06bd
97bcf97c3598082c95f8c965cc920f
7f0e37f0e37f14898082b0723b02d5
97bcf97c3598082c95f8e1cfcc920f
RWRmHuT9PSqtwfsLtEx+QS06BJtLgFYteL9WCNjH7yuyu5Y1DieSN7lf
6438bc162a5dc9ff33dfec5faf377e54747c42626e9664c1127bfc70d2e5033a
9778397bd197c36c9210c9274c91aa
5c3ed1dae51d4543805ea48d
97bcf7f0e47f531b0b0bb0b6fb0722
97b6b97bd19801ec95f8c965cc920e
0123456789ABCDEFGHJKLMNPQRTUWXY
9778397bd097c36b0b6fc9210c91aa
9778397bd097c36c9210c9274c920e
97bd07f1487f595b0b0bc920fb0722
97bd0b06bdb0722c965ce1cfcc920f
9778397bd097c36b0b6fc9210c8dc2
fff201a34e823e204843835134e8f2e6b122d4521db3ad35daa8e1fe60a343fa
7f07e7f0e37f14998082b0787b0721
97bcf7f1487f595b0b0bb0b6fb0722
7f0e37f1487f531b0b0bb0b6fb0722
97bd097bd097c35c0b6fc920fb0722
97b6b7f0e47f149b0723b0787b0721
9778397bd097c36b0b70c9274c91aa
7f0e27f0e47f531b0723b0b6fb0722
49d2147716ff75a90a3c98aff02381780
97bd09801d98082c95f8e1cfcc920f

免责声明及风险提示:

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。