南明离火
移动应用检测平台

ANDROID 静态分析报告

SuperCard X • v11.1.1

分析日期: 2025-04-03 23:22:19

应用概览

文件名称:	SuperCard X_11.1.1 pos_m_sign.apk
文件大小:	21.64MB
应用名称:	SuperCard X
软件包名:	io.dxpay.remotenfc.SuperCard1
主活动:	io.dxpay.remotenfc.SuperCard.gui.LoginActivity
版本号:	11.1.1
最小SDK:	26
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:	56/100 (中风险)
杀软检测:	经检测，该文件安全
MD5:	90e0e6ebcea81f0beb106dee42ca58f9
SHA1:	d7890411ff36304457f3b09ae50572248415c9cfe
SHA256:	331de31f0862980f9609b8f6a1db7585ac23bea567bc4de6b7f74bcf0dadfcf

分析结果严重性

高危	中危	信息	安全	关注
1	12	2	2	1

四大组件信息

Activity组件：7个，其中export的有：2个
Service组件：2个，其中export的有：1个
Receiver组件：1个，其中export的有：1个
Provider组件：2个，其中export的有：0个

证书信息

二进制文件已签名
v1 签名: False

v2 签名: True
v3 签名: False
v4 签名: False
主题: C=Us, ST=android, L=android, O=android, OU=android, CN=android
签名算法: rsassa_pkcs1v15
有效期自: 2025-03-26 05:48:33+00:00
有效期至: 2049-03-20 05:48:33+00:00
发行人: C=Us, ST=android, L=android, O=android, OU=android, CN=android
序列号: 0x3afd41e8
哈希算法: sha512
证书MD5: 327c898597b5efa2c3ddff87f3ba33a7
证书SHA1: 6ffeec80a4df929ac68cad611fa1dc65c1cbec66
证书SHA256: 6ab4cf6ad97b1987b7be1d8026e71f92f3f12e4aa3554669b2e0257b2dbf8e73
证书SHA512:
1f77d33f9b20a9ead7f2798141d916641883af4d2e3c673ba8069f36536a98e27aff321a7063d7cef6ea291c30a92d305c357c54e50737b3309633398db81d5

公钥算法: rsa
密钥长度: 2048
指纹: 13bba1410d018cb6f3178c5c3afe92cfaffce8237d380c8aa31840e3dc798fea
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.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。
android.permission.NFC	危险	控制nfc功能	允许应用程序与支持nfc的物体交互。
android.permission.BIND_NFC_SERVICE	签名	系统绑定到 NFC 服务所需的	必须由HostApduService 或要求OffHostApduService以确保只有系统可以绑定到它。
android.permission.CHANGE_NFC_STATE	未知	未知权限	来自 android 引用的未知权限。
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.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.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.FOREGROUND_SERVICE_CONNECTED_DEVICE	普通	通过连接的设备使用启用前台服务	允许常规应用程序使用类型为“connectedDevice”的 Service.startForeground。
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.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.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.DOWNLOAD_WITHOUT_NOTIFICATION	普通	后台下载文件	这个权限是允许应用通过下载管理器下载文件，且不对用户进行任何提示。
io.dxpay.tmotenfc.SuperCard.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
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。

本报告由南明离火移动安全分析平台生成

可浏览的Activity组件

ACTIVITY	INTENT
io.dxpay.remotenfc.SuperCard.gui.DeepLinkHandlerActivity	Schemes: app://, Hosts: supercard.plus,
io.dxpay.remotenfc.SuperCard.gui.MainActivity	Schemes: http://, https://, Hosts: supercard.plus, Mime Types: application/*,

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: **0** | 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: **5** | 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	应用程序可以使用明文网络流量，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	Activity (io.dxpay.remotenfc.SuperCard.gui.DeepLinkHandlerActivity) 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。
3	Activity (io.dxpay.remotenfc.SuperCard.gui.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	Service (io.dxpay.remotenfc.SuperCard.nfc.hce.ApduService) 受权限保护，但是应该检查权限的保护级别。 Permission: android.permission.BIND_NFC_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。

5	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。

安全漏洞检测

高危: **1** | 警告: **6** | 信息: **2** | 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
3	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
4	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	警告	OWASP MASVS: MSTG-STORAGE-10	升级会员：解锁高级权限
5	该文件是World Readable。任何应用程序都可以读取文件	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
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	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

8	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
9	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
10	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

行为分析

编号	行为	标签	文件
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
00189	获取短信内容	短信	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
00126	读取敏感数据（短信、通话记录等）	信息收集 短信 通话记录 日历	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
00188	获取短信地址	短信	升级会员：解锁高级权限
00011	从 URI 查询数据（SMS、CALLLOGS）	短信 通话记录 信息收集	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
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
00163	创建新的 Socket 并连接到它	socket	升级会员：解锁高级权限
00162	创建 InetSocketAddress 对象并连接到它	socket	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
00013	读取文件并将其放入流中	文件	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

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
00026	方法反射	反射	升级会员：解锁高级权限
00161	对可访问性节点信息执行可访问性服务操作	无障碍服务	升级会员：解锁高级权限
00173	获取 AccessibilityNodeInfo 屏幕中的边界并执行操作	无障碍服务	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

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.REQUEST_INSTALL_PACKAGES android.permission.CAMERA
其它常用权限	5/46	android.permission.ACCESS_WIFI_STATE android.permission.FOREGROUND_SERVICE android.permission.ACCESS_NETWORK_STATE android.permission.CHANGE_WIFI_STATE 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。

域名检测

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
super-card-sschh.com	安全	是	**IP地址:** 38.47.213.197 **国家:** 中国 **地区:** 香港 **城市:** 香港 **纬度:** 22.285521 **经度:** 114.157692 **查看:** 高德地图
t.me	安全	否	**IP地址:** 149.154.167.99 **国家:** 大不列颠及北爱尔兰联合王国 **地区:** 英格兰 **城市:** 伦敦 **纬度:** 51.508530 **经度:** -0.125740 **查看:** Google 地图

URL链接分析

URL信息	源码文件
• https://super-card.rcchh.com/	io/dxpay/remotenfc/SuperCard/global/SuperApplication.java
• https://t.me/supercard_x	q1/m.java
• https://www.google.com	io/dxpay/remotenfc/SuperCard/gui/LoginActivity.java
• https://github.com/supabase-community/supabase-kt/wiki/session-saving	f1/H.java
• https://ktor.io/docs/http-client-engines.html	V1/d.java
• https://ktor.io/docs/faq.html#no-transformation-found-exception	V1/d.java

第三方SDK

SDK名称	开发者	描述信息
ZXing Android Embedded	JourneyApps	Barcode scanning library for Android, using ZXing for decoding.
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。
Jetpack ProfileInstaller	Google	让库能够提前预填充要由 ART 虚拟机的编译轨迹。
Jetpack Room	Google	Room 持久性库在 SQLite 的基础上提供了一个抽象层，让用户能够在充分利用 SQLite 的强大功能的同时，获享更强健的数据库访问机制。

密钥凭证

可能的密钥
"login_password": "Password"
"private_server": "Private"
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
eyJpc3MiOiJzdXBhYmFzZSIsInJlZiI6ImFoZnh4aXRoamFzZ29lb3hqdXhuIiwicm9sZSI6ImFub24iLCJpYXQiOjE3MzkyMDQyNjEsImV4cCI6MjA1NDc4MDI2MX0
59ebfcb9a4cb94ecc5cf04b9a6cce1a
2858dd39e7c190fcae137a225c423b6
uIZJK5Y6tHZxIBrziCO4UAZm9dnhGcpVmOfmAef2c5o

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，深入扫描软件中中潜在的漏洞和安全隐隐患。