Evaluation Warning: The document was created with Spire.Doc for Python.

**OTAupgrade（ 22.1.2.05版本）
APK分析报告**

## **1. 分析结果概述**

**说明：本分析结果由摸瓜网站自动生成，一共包含以下10类内容：（1）分析结果概述（2）APK文件基本信息（3）APP基本信息（4）线索情况（5）签名证书（6）硬编码敏感信息（7）加壳分析（8）第三方插件（9）此APP的危险动作（10）应用内通信。
\*此分析结果仅供参考，请勿商用。\*。**

| 类别 | 内容 |
| --- | --- |
| APP名称 | OTAupgrade |
| 版本 | 22.1.2.05 |
| 包名 | com.changhong.upgrade |
| 域名线索 | 2条 |
| URL线索 | 2条 |
| APP图标 |  |
| 分析日期 | 2025年6月30日 |
| 分析平台 | [摸瓜APK反编译平台](https://mogua.co) |

## **2. APK文件基本信息**

| 类别 | 内容 |
| --- | --- |
| 文件名 | CH\_UpgradeOTA\_22.1.2.05\_220104\_signed.apk |
| 文件大小 | 4.12MB |
| MD5值 | e664c387f01d14eb21c1114ce27922b2 |
| SHA1值 | 71a76004b3829cd17907d61265d72188c7aba754 |
| SHA256值 | 759ef84aea13d31ff1038aec0cc1099a3323026b877ee14563f18c5ae8045408 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | OTAupgrade |
| 包名 | com.changhong.upgrade |
| 主活动Activity |  |
| 安卓版本名称 | 22.1.2.05 |
| 安卓版本 | 2 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| 192.168.1.145 | IP: 192.168.1.145 所属国家: - 地区: - 城市: -  |
| 10.9.46.21 | IP: 10.9.46.21 所属国家: - 地区: - 城市: -  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://192.168.1.145:8080/iho-3000/config.txt  | com/changhong/upgrade/transfer/TscDownConfigFile.java  |
| http://10.9.46.21:8080/test/update02.zip  | Mogua Engine V1  |

### **4.3 邮箱线索**

### **4.4 手机号线索**

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: True v3 签名: False 找到 1 个唯一证书 主题: C=CN, ST=SiChuan, L=MianYang View, O=Android, OU=Android, CN=Android, E=android@android.com 签名算法: rsassa\_pkcs1v15 有效期自: 2017-09-04 04:21:02+00:00 有效期至: 2045-01-20 04:21:02+00:00 发行人: C=CN, ST=SiChuan, L=MianYang View, O=Android, OU=Android, CN=Android, E=android@android.com 序列号: 0xd40ccd2966ec22b1 哈希算法: sha1 md5值: 9f7bf51a3481a43ef731c0c43ea499e7 sha1值: 686868f186f47c14087bc8c26996f37bb3651e76 sha256值: f5ac980c5c1a66ad98b8a327830ce248c247e3d52f4e3feb1243b319656d93b8 sha512值: dc375afd67abaaf58fd5ec688bf97557f1a6216149307a34294b18586327900580dc2f58f7d46a78cac1eb67d6c73e63770f6e8f53203f0d8d3cbd28e478b82b 公钥算法: rsa 密钥长度: 2048 指纹: 21a044fb02cb8bb74fcc0c6ba4671b6635350403c101188be80f67c5d88287a7**

## **6. 硬编码敏感信息**

## **7. 加壳分析**

| 加壳类型 | 所属文件 |
| --- | --- |
| 登陆摸瓜网站后查看  |  |

## **8. 第三方插件**

| 名称 | 分类 | URL链接 |
| --- | --- | --- |
| 登陆摸瓜网站后查看  |  |  |

## **9. 此APP的危险动作**

| 向手机申请的权限 | 是否危险 | 类型  | 详细情况 |
| --- | --- | --- | --- |
| android.permission.RECEIVE\_BOOT\_COMPLETED | 正常 | 开机时自动启动 | 允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度 |
| android.permission.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| android.permission.ACCESS\_WIFI\_STATE | 正常 | 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 | 正常 | 查看网络状态 | 允许应用程序查看所有网络的状态 |
| android.permission.SYSTEM\_ALERT\_WINDOW | 危险 | 显示系统级警报 | 允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕 |
| android.permission.READ\_EXTERNAL\_STORAGE | 危险 | 读取外部存储器内容 | 允许应用程序从外部存储读取 |
| 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 |

## **10. 应用内通信**

**报告由**  [**摸瓜APK反编译平台**](https://mogua.co)  **自动生成，并非包含所有检测结果，有疑问请联系管理员。**