预警编号：YJ-2018004

恒安嘉新

关于多款 Android 平台 WebView 控件

存在跨域访问高危漏洞

安全预警通告

恒安嘉新（北京）科技股份公司

2018 年 1 月 10 日

1 漏洞描述

近期，互联网爆出 Android WebView 存在跨域访问漏洞。攻击者利用该漏洞，可远程获取用户隐私数据（包括手机应用数据、照片、文档等敏感信息），还可窃取用户登录凭证，在受害者毫无察觉的情况下实现对 APP 用户账户的完全控制。由于该组件广泛应用于 Android 平台，导致大量 APP 受影响，构成较为严重的攻击威胁。该漏洞危害程度为高危(High)。

2 影响范围

漏洞影响使用 WebView 控件，开启 file 域访问并且未按安全策略开发的 Android 应用 APP。

3 漏洞原理

WebView 是 Android 用于显示网页的控件，是一个基于 Webkit 引擎、展现 web 页面的控件。WebView 控件功能除了具有一般 View 的属性和设置外，还可对 URL 请求、页面加载、渲染、页面交互进行处理。

该漏洞产生的原因是在 Android 应用中，WebView 开启了 file 域访问，允许 file 域访问 http 域，且未对 file 域的路径进行严格限制所致。攻击者通过 URL Scheme 的方式，可远程打开并加载恶意 HTML 文件，远程获取 APP 中包括用户登录凭证在内的所有本地敏感数据。

漏洞触发成功前提条件如下：

1.WebView 中 setAllowFileAccessFromFileURLs 或 setAllowUniversal AccessFromFileURLsAPI 配置为 true；

2.WebView 可以直接被外部调用，并能够加载外部可控的 HTML 文件。

4 修复建议

厂商暂未发布解决方案，可以先采用以下临时解决方案：

1. file 域访问为非功能需求时，手动配置 setAllowFileAccessFromFileURLs 或 setAllowUniversalAccessFromFileURLs 两个 API 为 false。（Android4.1 版本之前这两个 API 默认是 true，需要显式设置为 false）

2. 若需要开启 file 域访问，则设置 file 路径的白名单，严格控制 file 域的访问范围，具体如下：

（1）固定不变的 HTML 文件可以放在 assets 或 res 目录下，file:///android_asset 和 file:///android_res 在不开启 API 的情况下也可以访问；

（2）可能会更新的 HTML 文件放在/data/data/(app) 目录下，避免被第三方替换或修改；

（3）对 file 域请求做白名单限制时，需要对“../../”特殊情况进行处理，避免白名单被绕过。

3. 避免 App 内部的 WebView 被不信任的第三方调用。排查内置 WebView 的 Activity 是否被导出、必须导出的 Activity 是否会通过参数传递调起内置的 WebView 等。

4. 建议进一步对 APP 目录下的敏感数据进行保护。客户端 APP 应用设备相关信息（如 IMEI、IMSI、Android_id 等）作为密钥对敏感数据进行加密。使攻击者难以利用相关漏洞获得敏感信息。