预警编号：YJ-2018006

恒安嘉新

关于 OAuth 2.0 存在第三方帐号快捷登录授权劫持漏洞

安全预警通告

恒安嘉新（北京）科技股份公司

2018 年 1 月 23 日

1 漏洞描述

近期，互联网爆出 OAuth 2.0 存在第三方帐号快捷登录授权劫持漏洞。综合利用上述漏洞，攻击者可通过登录受害者账号，获取存储在第三方移动应用上的敏感信息。由于 OAuth 广泛应用于微博等社交网络服务，漏洞一旦被黑客组织利用，可能导致用户隐私信息泄露。该漏洞危害程度为中危。

2 影响范围

上述漏洞影响采用第三方登陆授权方式的服务。

3 漏洞原理

OAuth（Open Authorization）是一个关于授权的开放网络标准，允许用户授权第三方移动应用，访问用户存储在其他服务提供者上的信息，而无需将用户名和密码提供给第三方移动应用或分享数据的所有内容。

该漏洞利用 OAuth 第三方授权无需用户名和密码的特点，结合 redirect_uri 未指定授权目录引发用户劫持攻击。攻击者通过登录某种社交网络服务，修改链接 redirect_uri 参数值指向，将伪造后的用户授权链接发给目标用户，当目标用户点击或被欺骗访问上述授权链接进行登陆后，攻击者即可通过 referer 获取用户授权，快速登录目标用户账号，还可登陆该账号绑定的其他网站信息，查看敏感信息或执行授权操作，还可以利用受害人账号进行非法信息传播、诈骗等非法行为。

4 修复建议

建议第三方应用平台采取如下措施进行漏洞的防范,同时请广大用户注意第三方授权链接，谨慎输入账号密码：：

1. 在注册第三方授权时，redirect_uri 需要限制到指定网站的指定目录，比如 redirect_uri 注册为 passport.aaa.com/oauth/，而非 aaa.com 或者 passport.aaa.com。

2. 禁止非源跳转。通过增加网站跳转的判断条件，禁止对非本网站的链接进行跳转。