

漏洞概要

关注数(12) [关注此漏洞](#)缺陷编号：[WooYun-2012-11104](#)

漏洞标题：淘网址sina oauth认证登录漏洞

相关厂商：[淘宝网](#)漏洞作者：[Tom](#)

提交时间：2012-08-24 15:49






公开时间：2012-10-08 15:50

漏洞类型：设计缺陷/逻辑错误

危害等级：中

自评Rank：8

漏洞状态：厂商已经确认

漏洞来源：<http://www.wooyun.org>，如有疑问或需要帮助请联系 help@wooyun.orgTags标签：[设计缺陷/边界绕过](#) [设计错误](#) [逻辑错误](#) [认证绕过](#) [欺骗登陆](#)分享漏洞：     2

2人收藏

[收藏](#)

漏洞详情

披露状态：

- 2012-08-24：细节已通知厂商并且等待厂商处理中
- 2012-08-24：厂商已经确认，细节仅向厂商公开
- 2012-09-03：细节向核心白帽子及相关领域专家公开
- 2012-09-13：细节向普通白帽子公开
- 2012-09-23：细节向实习白帽子公开
- 2012-10-08：细节向公众公开

简要描述：

网站登录系统存在漏洞,可以不经授权登录别人帐号

详细说明：

登录系统时的微博登录方式

微博帐号验证成功后返回跳转网址

`http://i.tao123.com/sina_login.php?jump=http://i.tao123.com/#access_token=xxxxxxxxxxxx&remind_in=*****&expires_in=*****&uid=*****`

只要更换后面的uid 如果这个帐号ID在网站存在 网站则会授权登录访问此帐号

漏洞证明：

跳转后未对授权代码做验证 只验证了 token是否有效 并未验证和uid的对应关系



修复方案：

版权声明：转载请注明来源 [Tom@乌云](#)

漏洞回应

厂商回应：

危害等级：中

漏洞Rank：8

确认时间：2012-08-24 15:51

厂商回复：

非常感谢Tom对淘宝安全的关注和支持，此问题已处理

最新状态：

暂无

漏洞评价：

对本漏洞信息进行评价，以更好的反馈信息的价值，包括信息客观性，内容是否完整以及是否具备学习价值

漏洞评价(共0人评价)：

登录后才能进行评分

评价

2012-08-24 15:57 king (路人 Rank:15 漏洞数:2 喜爱安全，网络游戏安全应用漏洞挖掘)	0
私密的安全问题也越来越有意思了！！	1#
2012-09-13 17:23 horseluke (普通白帽子 Rank:116 漏洞数:18 Realize the dream in earnest.)	0
这个bug非常有意思！第三方的关联验证问题确实很容易犯~	2#
2012-09-13 17:26 horseluke (普通白帽子 Rank:116 漏洞数:18 Realize the dream in earnest.)	0
缺陷关联： WooYun: 5sing.com借助第三方连接可创建重复昵称账户 (第三方登录的关联验证常见问题)	3#

登录后才能发表评论，请先 [登录](#)。