淮安市生态环境局

渗透测试报告



淮安易云科技有限公司

### Swagger Api 接口未授权访问（中）\*2

**漏洞描述**

Swagger 是一个将 Pure FlashArray和FlashBlade API 文档提供到流行的交互式 Swagger UI 中的工具。 Swagger 存在安全漏洞，其配置文件可能在权限控制不当的情况下被攻击者直接访问。

**漏洞细节**

**污染源国发平台**

<http://10.203.24.44:17088/v2/api-docs>

<http://10.203.24.43:18088/v2/api-docs>



**修复方案**

1.隐藏 module 信息：修改配置文件 list =false。

2.权限控制：不需要写入权限的 module 的设置为只读 Read only = true;

3.网络访问控制：使用安全组策略或白名单限制，只允许必要访问的主机访问;

4.账户认证：只允许指定的用户利用指定的密码使用 rsync 服务;

## 安全建议

随着越来越多的网络访问通过Web界面进行操作，Web安全已经成为互联网安全的一个热点，基于Web的攻击广为流行，SQL注入、跨站脚本等Web应用层漏洞的存在使得网站沦陷、页面篡改、网页挂马等攻击行为困扰着网站管理者并威胁着网站以及直接用户的安全。基于此，我们可从如下几个方面来消除这些风险，做到防患于未然：

1. 对网站的开发人员进行安全编码方面的培训，在开发过程避免漏洞的引入能起到事半功倍的效果。

2. 请专业的安全研究人员或安全公司对架构网站的程序和代码做全面的源码审计，修补所有发现的安全漏洞，这种白盒安全测试比较全面、深入，能发现绝大部分的安全问题。

3. 在网站上线前，使用Web应用漏洞扫描系统进行安全评估，并修补发现的问题；在网站上线后，坚持更新并使用网站安全监测系统，对整站以及关键页面进行周期和实时监测，及时消除发现的隐患。

4. 采用专业的Web安全防火墙产品，可以在不修改网站本身的情况下对大多数的Web攻击起到有效的阻断作用。

5. 建议网络管理员、系统管理员、安全管理员关注安全信息、安全动态及最新的严重漏洞，特别是影响到Web站点所使用的系统和软件的漏洞，应该在事前设计好应对规划，一旦发现系统受漏洞影响及时采取措施。