CVE-2020-13390: Tenda Vulnerability

Vendor of the products: Tenda Reported by: Joel CVE details Affected products:

1 AC9 V1.0 V15.03.05.19(6318) CN 2 AC9 V3.0 V15.03.06.42 multi 3 AC15 V1.0 V15.03.05.19 multi TD01 4 AC18 V15.03.05.19(6318) CN 5 AC6 V1.0 V15.03.05.19_multi_TD01

An issue was discovered on Tenda AC6 V1.0 V15.03.05.19_multi_TD01, AC9 V1.0 V15.03.05.19(6318), AC9 V3.0 V15.03.06.42_multi, AC15 V1.0 V15.03.05.19_multi_TD01, AC18 V15.03.05.19(6318) devices. There is a buffer overflow vulnerability in the router's web server—httpd. While processing the entrys and mitinterface parameters for a post request, the value is directly used in a sprint to a local variable placed on the stack, which overflows the return address of the function. The attackers can construct a psyload to carry out arbitrary code attacks.

POC

This PoC can result in a Dos.

Given the vendor's security, we only provide parts of the HTTP.

```
1 FOST /goform/addressMat HTTF/1.1
2 Most: 192.66.10.131
3 Most: 192.66.10.131
4 X-Requested-with: SWLMittpRequest
5 User-Apont: Mocilia/5.0 (Macintosh) Intel Mac OS x 10_14_5) AppleMebEit/537.36 (KMTMIL, like Gecko) Chrome/75.0.3770.100 Safari/537.36
5 User-Apont: Mocilia/5.0 (Macintosh) Intel Mac OS x 10_14_5) AppleMebEit/537.36 (KMTMIL, like Gecko) Chrome/75.0.3770.100 Safari/537.36
8 Accept-Encoding: gript, defined-formusiencoded
8 Accept-Encoding: gript, defined-formusiencoded
9 Accept-Encoding: gript, defined-formusiencoded
10 Connection: (close/plain)
11 Cookie: passord=mbf5gk
```

Details

ARM

```
__fastcall fromAddressNat(int a1)
      void *v1; // r0
int v2; // r0
int v3; // r0
int v4; // [sp+ch] [bp-420h]
int v5; // [sp+14h] [bp-418h]
char s; // [sp+14h] [bp-318h]
char v5; // [sp+314h] [bp-18h]
void *v8; // [sp+414h] [bp-18h]
void *v8; // [sp+414h] [bp-14h]
void *v9; // [sp+414h] [bp-14h]
void *v10; // [sp+41ch] [bp-14h]
| vd = al;
| memset(&v5, 0, 0x100u);
| vi0 = get_param(vd, (int)*entrys*, (int)&unk_E41FC);
| vi0 = get_param(vd, (int)*mitInterface*, (int)&unk_E41FC);
| sprintf(&v. "Ss_5*s. vd), vo);
| sub_de5cc((int)*adv.addrnat*, &s, 0x7Eu);
| vt = get_param(vd, (int)*page*, (int)**1*);
| v0 = v1;
| v1 = get_param(vd, (int)*page*, (int)**1*);
| v2 = sprintf(&v7, "advance/addressNatList.asp?page=%s*, v1);
| if (CommitCfm(v2))
        {
    sprintf((char *)&v5, "advance_type=%d", 7);
    send_msg_to_netctrl(5, &v5);
            return sub_2BD94(v4, &v7);
```

MIPS

```
| Sg., 86330-cm £OR(Mg) | In Sg., 86430-cm £OR(M
                                                                                                                                                                                                                                                                         | 500, 0x450+xxx _200(5/p) | 501, 0x450+xxx _200(5/p) | 502, 0x450+xxx _200(5/p) | 502, 0x450+xxx _200(5/p) | 502, 0x450+xxx _200(5/p) | 502, 0x450+xx _200(5/p) | 502, 0x
                                                                                                                                                                                                                                                          $17. methodram (AD($fp) $00, mother (fp) $00, mother (finder($fp) $00, mother (finder($fp) $00, mother (finder($fp) $00, mother (finder($fp) $00, mother (finder) $00, mother (fi
                                                              rop

100 Sgp, McAS6var A20(Sfp)

abblu 100, Sfp, McAS0-Llat

1 501, McAS0-Llat

1 501, McAS0-Llat

abblu 560, 501, (absheddrest_0 - 0x510000) s "abs.abbrast"

move bal. 100 s bull
```

Posted by Joel vulnerability

Tweet

« CVE-2020-13389: Tenda Vulnerability CVE-2020-13391: Tenda Vulnerability »



About Me



To see what I'm working on, check out my GitHub page here.

Recent Posts

CVE-2020-13390: Tenda Vulnerability

GitHub Repos

joel-malwarebenchmark_github.io
 @joel-malwarebenchmark_on GitHub

Copyright © 2020 - Joel - Powered by <u>Octopress</u>