

tp-link TL-WR841N V14

Firmware frissítések útvesztőjében.

A tp-link tl-wr841n típusú router egy rendkívül népszerű router az otthoni felhasználók körében, mi sem bizonyítja ezt jobban, hogy a router már a 14-ik hardware verziónál tart. Népszerűségének oka az alacsony ár fekvésében, valamint a könnyű konfigurálhatóságában rejlik.

Az elmúlt években számos alkalommal fedeztek fel a router különböző verzióiban olyan sérülékenységeket, amely jogosulatlan távoli kód futtatást eredményezhet az eszközön. Mit jelent ez a gyakorlatban? A sérülékenység sikeres kihasználását követően a támadó operációs rendszer szintű hozzáféréssel, adminisztrátori jogosultsággal rendelkezik a hálózati eszköz felett és így pedig jó eséllyel a teljes hálózati forgalom felett is. Ilyen sérülékenységek a közelmúltból például a CVE-2022-30024 és CVE-2020-8423. Ezek a sérülékenységek távoli kód futtatást tesznek lehetővé a tp-link tl-wr841n típusú routereken.

Amiért ez a kis írás valójában elkészült, annak az oka az, hogy a fent említett két sérülékenység a router nem minden hardware verzióját érintette!

CVE-2022-30024 sérülékenységben érintett hardware verziók:

V12 TL-WR841N(EU)_V12_160624

V11 TL-WR841N(EU)_V11_160325

V11 TL-WR841N_V11_150616

V10 TL-WR841N_V10_150310

CVE-2020-8423 sérülékenységben érintett hardware verziók:

V10 TL-WR841N

Tehát ahogy az elején említettük, ez a router jelenleg a 14-es hardware verziónál tart, így bár van létjogosultsága a fenti sérülékenységeknek hiszen bőven lehetnek még használatban ezek közül a hardware verziók közül, mégsem beszélhetünk a legfrissebb hardware verzióban kihasználható sérülékenységekről, márpedig, ha valaki 2022-ben egy ilyen routert szeretne bármilyen okból, akkor a V14-es verziót fogja tudni megvásárolni. Nekünk pedig több se kellett, elkezdtünk utána járni, hogy bárki az elmúlt években jelentett e sérülékenységet a V14-es verzióban és mivel nem találtunk egyetlen publikus hibajelentést sem, ami a V14-es hardware verzió sérülékenységről tett volna említést, így hát rendeltünk magunknak egyet, hogy megvizsgáljuk és megpróbáljunk hasonló sérülékenységet találni a V14 hardware verzióban is. Az elsődleges cél, hogy LAN oldali távoli kód futtatásra alkalmas sérülékenységet találjunk, lehetőség szerint olyat, amihez nem szükséges autentikáció, tehát egy Pre-auth RCE kihasználás építhető.

Miután megérkezett az eszköz, az első dolgunk az volt, hogy ellenőrizzük milyen hardware verziót küldtek, ugyanis az online rendelési felületen nem volt lehetőség hardware verziót választani. Ahogy sejtettük természetesen a V14 verziót kaptuk.



Rögtön neki is láttunk a router vizsgálatának! Az első dolog, amit megnéztünk az elérhető hálózati szolgáltatások listája volt.

```
C:\Users\pappe>nmap -sV -PN -p1-65535 192.168.0.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-26 16:22 Kézűp-eurpai nyári idő
Nmap scan report for 192.168.0.1
Host is up (0.0039s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      Dropbear sshd 2012.55 (protocol 2.0)
80/tcp    open  http
1900/tcp   open  upnp     Portable SDK for UPnP devices 1.6.19 (Linux 2.6.36; UPnP 1.0)
```

```
C:\Users\pappe>nmap -sU -PN 192.168.0.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-26 17:09 K÷zúp-eur~pai nyßri id$
Warning: 192.168.0.1 giving up on port because retransmission cap hit (10).
Nmap scan report for 192.168.0.1
Host is up (0.0014s latency).
Not shown: 992 closed udp ports (port-unreach)
PORT      STATE      SERVICE
67/udp    open|filtered dhcp
1900/udp   open       upnp
23557/udp  open|filtered unknown
34038/udp  open|filtered unknown
39714/udp  open|filtered unknown
41524/udp  open|filtered unknown
46836/udp  open|filtered unknown
51554/udp  open|filtered unknown
MAC Address: 5C:A6:E6:6F:B7:66 (TP-Link Limited)

Nmap done: 1 IP address (1 host up) scanned in 1649.26 seconds
```

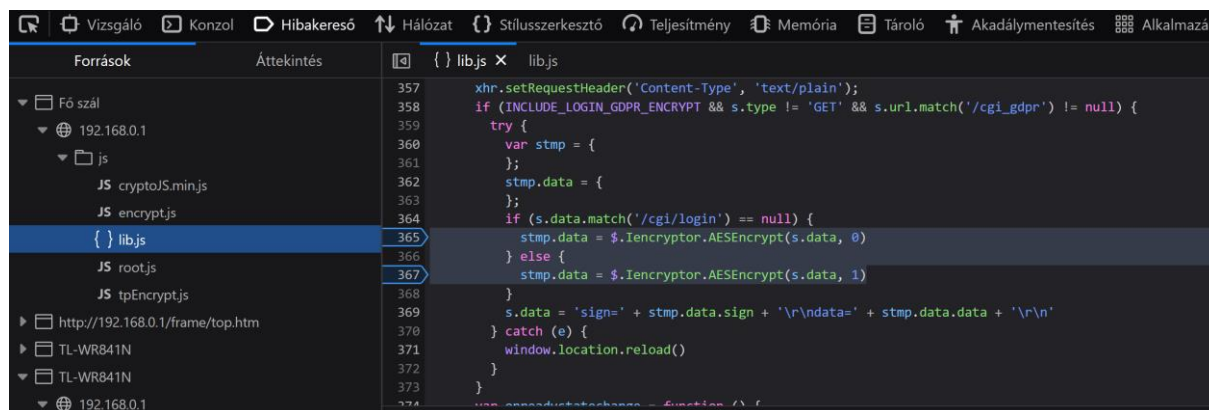
Ezek alapján a mi szempontunkból, ami érdekes lehet az a **http** és **upnp** szolgáltatás, a **httpd** binárisnak számos funkciót kell megvalósítania és számos a felhasználótól érkező adatot kell kezelnie, így potenciálisan nagyobb a lehetősége, hogy a kódban valamilyen hibát találjunk. Az **upnp** protokoll pedig mivel nem valósít meg hitelesítést így, ha az **upnpd** binárisban találunk sérülékenységet az mindenképpen jackpot hiszen nem kell bajlódni a hitelesítés megkerülésével, viszont az **upnp** esetén lényegesen kevesebb a megvalósítandó funkció és a felhasználótól érkező adat, amit a kódnak kezelnie kell így némileg a hiba lehetőség is kevesebb.

Úgy döntöttünk, hogy első körben elkezdjük megvizsgálni a **http** szolgáltatást. A webes adminisztrátori felület megnyitásakor egyértelművé vált, hogy ez a "klasszikus" tp-link felhasználói felület amit a tp-link talán a legrégebb óta használ kisebb nagyobb módosításokkal az elmúlt években (Az újabb, magasabb ár fekvésű modellek új adminisztrátori felületet kaptak.).

The screenshot displays the TP-Link Wireless N Router WR841N web interface. The main content area is divided into sections for Status, LAN, and Wireless 2.4GHz. The LAN section shows the router's IP address as 192.168.0.1 and its MAC address as 5C:A6:E6:6F:B7:66. The Wireless 2.4GHz section indicates that the wireless radio is enabled and the router is operating in Router mode. The left sidebar provides navigation options for various router settings, and the right sidebar offers help for the Status page.

Miután egy kicsit megvizsgáltuk a felhasználói felületet és hogy miképpen küldi az adatokat a böngésző a **http** szervernek, rájöttünk, hogy ez a firmware verzió még a régebbi titkosítási

eljárást használja. Az újabb firmware verziókban némileg összetettebb és bonyolultabb eljárások mentén van megvalósítva a http szervernek küldött adatok titkosítása.

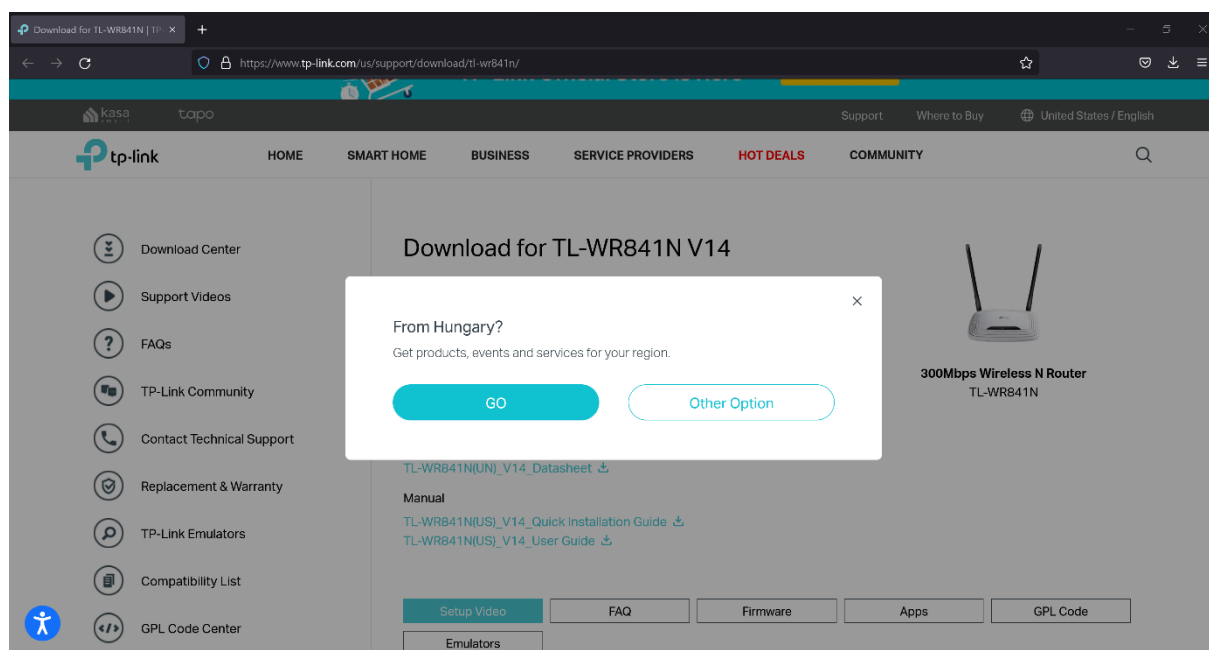


```
357 xhr.setRequestHeader('Content-Type', 'text/plain');
358 if (INCLUDE_LOGIN_GDPR_ENCRYPT && s.type != 'GET' && s.url.match('/cgi_gdpr') != null) {
359   try {
360     var stmp = {
361     };
362     stmp.data = {
363     };
364     if (s.data.match('/cgi/login') == null) {
365       stmp.data = $.Iencryptor.AESEncrypt(s.data, 0)
366     } else {
367       stmp.data = $.Iencryptor.AESEncrypt(s.data, 1)
368     }
369     s.data = 'sign=' + stmp.data.sign + '\r\ndata=' + stmp.data.data + '\r\n'
370   } catch (e) {
371     window.location.reload()
372   }
373 }
374 var encryptdata = function () {
```

Az eddigiek alapján nagyon úgy tűnik, hogy ez a firmware pontosan ugyanazt a jól ismert **httpd** binárist futtatja és ugyan azt a függvény könyvtárat használja, amit számos egyéb más tp-link modell esetén is használt a gyártó és számos esetben azonosítottak benne sérülékenységet. Ilyen modell például a szintén közkedvelt **tp-link tl-wr840n**, valamint a **tp-link tl-wa801n AP**. Ez utóbbi modell esetében még az év elején azonosítottunk egy Post-auth **Buffer overflow** és szintén Post-auth **Command injection** sérülékenységet.

Viszont mivel korántsem biztos, hogy jelenleg a legfrissebb firmware verziót futtatja a routerünk, és mivel mi a legfrissebb firmware-t futtató legújabb hardware verzióban szeretnénk sérülékenységet találni, így ellátogattunk a gyártó oldalára, hogy információt szerezzünk az elérhető firmware verziókról és letöltsük a gyártó által kínált legfrissebb verziót.

A gyártó oldalát meglátogatva az oldal azt javasolja, hogy látogassuk meg a régióknak megfelelő tp-link oldalt.



A régióknak megfelelő oldalra átirányítást követően miután kiválasztottuk a hardware verziót nagy meglepetésünkre azt látjuk, hogy a routerünk a legfrissebb verziójú firmwaret futtatja, aminek kiadási dátuma 2020 11 27.

TL-WR841N(EU)_V14_200903		Letöltés
Kiadás dátuma: 2020-11-27	Nyelv: Angol	Fájl méret: 4.27 MB
Modifications and Bug Fixes: 1. Enhanced safety 2. Added the Led Control function 3. Added the WAN Link Status function 4. Optimized the wireless function 5. Optimized user experience of configuring the router		

Rendben, akkor töltsük le ezt a firmware-t és vizsgáljuk meg a **httpd** binárist, nézzük mit találunk a forráskódban. A firmware "kicsomagolásához" a Binwalk-ot használjuk.

```
(kali@kali)-[~/Downloads]
$ binwalk -Me TL-WR841Nv14_EU_0.9.1_4.17_up_boot[200903-rel58674].bin

Scan Time:      2022-08-26 16:30:41
Target File:    /home/kali/Downloads/TL-WR841Nv14_EU_0.9.1_4.17_up_boot[200903-rel58674].bin
MD5 Checksum:   7ade25cc4e706db227abd98b3b02f448
Signatures:     411

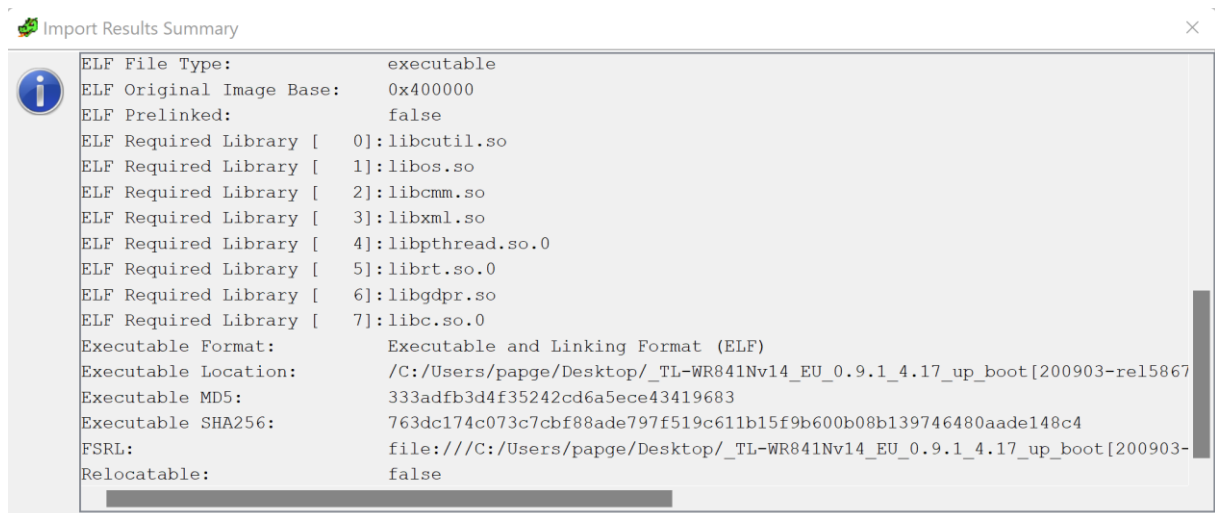
(kali@kali)-[~/Downloads/_TL-WR841Nv14_EU_0.9.1_4.17_up_boot[200903-rel58674].bin-0.extracted]
$ ls
100200.squashfs  10400  10400.7z  _10400.extracted  squashfs-root  squashfs-root-0

(kali@kali)-[~/Downloads/_TL-WR841Nv14_EU_0.9.1_4.17_up_boot[200903-rel58674].bin-0.extracted]
$ cd squashfs-root

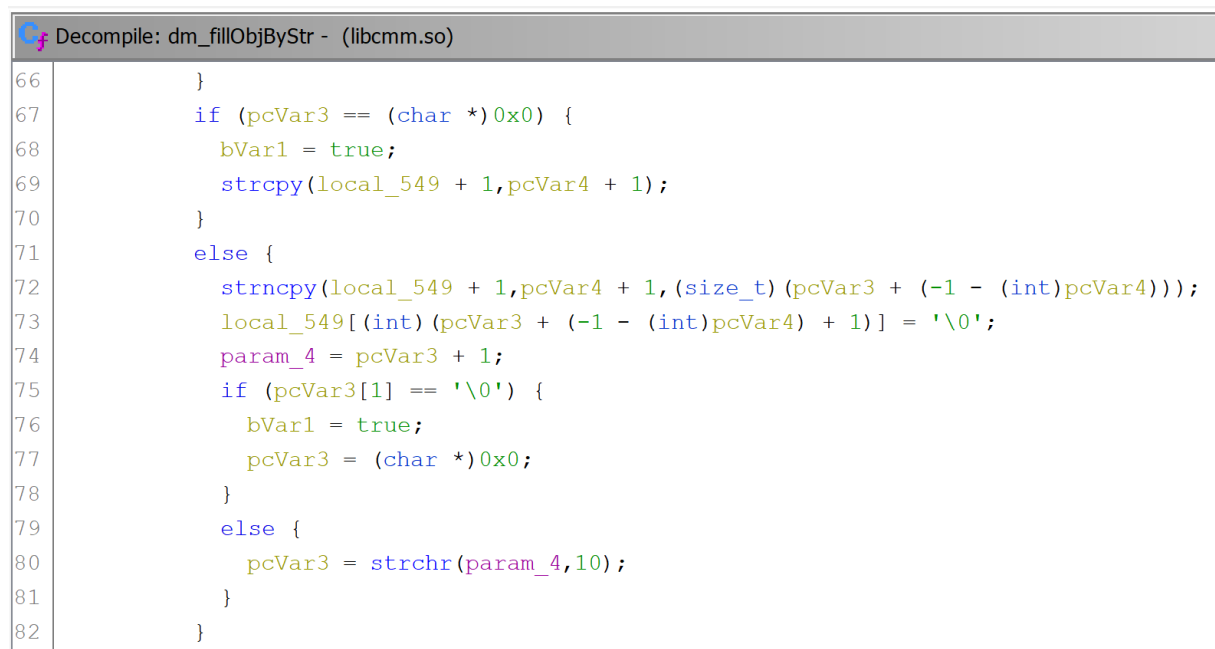
(kali@kali)-[~/Downloads/_TL-WR841Nv14_EU_0.9.1_4.17_up_boot[200903-rel58674].bin-0.extracted/squashfs-root]
$ ls
bin  dev  etc  lib  linuxrc  mnt  proc  sbin  sys  usr  var  web

(kali@kali)-[~/Downloads/_TL-WR841Nv14_EU_0.9.1_4.17_up_boot[200903-rel58674].bin-0.extracted/squashfs-root]
$
```

Most, hogy minden fájl rendelkezésünkre áll, vizsgáljuk meg a **httpd** binárist. A bináris visszafejtéséhez a Ghidra-t fogjuk használni. Miután megnyitjuk a **httpd** binárist a Ghidra-ban, azonnal láthatjuk, hogy milyen függvénykönyvtárakat használ.



Láthatjuk, hogy a **httpd** bináris több más függvény könyvtár mellett a jól ismert **libcmm.so** könyvtárat is használja, ez az a függvény könyvtár, amit a gyártó számos eszközének firmware-ében használ és a könyvtár egyes régebbi verzióiban a jól ismert overflow sérülékenységek találhatóak meg és használható ki. A sérülékenységek oka a **strcpy** és **strncpy** műveletek hibás használatából ered, ahogy az alábbi képen látható a nem megfelelő méret ellenőrzés vagy az ellenőrzés hiánya túlszorduláshoz vezet, ami potenciálisan kódfuttatást eredményezhet az érintett eszközön.



Most, hogy tudjuk, hogy a **httpd** bináris a sérülékeny **libcmm.so** függvény könyvtárat használja, könnyen demonstrálhatjuk a sérülékenységet. Ehhez nincs más dolgunk csak annyi, hogy a megfelelő helyen 1305 karakternél hosszabb karakterláncot küldjünk a **httpd** binárisnak. Természetesen kicsit többet szeretnénk látni abból, hogy mi történik az összeomlás alkalmával, így szükségünk lesz egy interaktív konzol hozzáférésre a debug környezet kialakításához. Ehhez pedig elsődlegesen a hardware-en található UART portot fogjuk használni.

Tehát a debug környezet ebben az esetben úgy épül fel, hogy az eszközön az UART porton interaktív konzol hozzáférést szereztünk ezután letöltöttük az eszközre a GDB debugger-t, majd elindítottuk a távoli hibakeresést. Így miután elküldjük a http szervernek a hibát kiváltó kérést, láthatjuk az alkalmazás összeomlását követő állapotot.

1) UART



2) GDB debugger.

```
(kali㉿kali)-[~]
└─$ gdb-multiarch
GNU gdb (Debian 12.1-3) 12.1
Copyright (C) 2022 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<https://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
  <http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word".
(gdb) set arch mips
The target architecture is set to "mips".
(gdb) set endian little
The target is set to little endian.
(gdb) target extended-remote 192.168.0.1:12345
Remote debugging using 192.168.0.1:12345
(gdb) attach 320
Attaching to process 320
warning: No executable has been specified and target does not support
determining executable automatically. Try using the "file" command.
0x2b6c85cc in ?? ()
(gdb)
```

3) Regiszterek állapota az összeomlás pillanatában

```
Program received signal SIGSEGV, Segmentation fault.
0x2affaf58 in ?? ()
(gdb) info registers
      zero      at      v0      v1      a0      a1      a2      a3
R0     00000000 00000001 00000a30 7f8727a8 7f871d78 fefefeff 00000000 00000000
      t0      t1      t2      t3      t4      t5      t6      t7
R8     00000041 00000000 00000000 00000000 00000000 00000000 00000000 00000000
      s0      s1      s2      s3      s4      s5      s6      s7
R16    7f871d78 41414141 7f8722e0 00000a30 7f872768 00000001 00000000 7f87673c
      t8      t9      k0      k1      gp      sp      s8      ra
R24    00000000 2b15e0c0 00000000 00000000 2b0614f0 7f871c90 7f8722e0 2affaf54
      status   lo      hi      badvaddr  cause   pc
      0100ff13 00000054 00000000 41414149 40800010 2affaf58
      fcsr     fir     hi1     lo1     hi2     lo2     hi3     lo3
      00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
      dspctl   restart
      00000000 00000000
```

```
Listing: libcmm.so_vuln
00087bc4 44 81 99 8f   lw      t9,-0x7ebc(gp)=>->strchr
00087bc8 21 20 20 02   move    param_1,s1
00087bcc 09 f8 20 03   jalr    t9=>strchr
00087bd0 0a 00 05 24   _li     param_2,0xa
00087bd4 20 00 bc 8f   lw      gp,local_590(sp)
00087bd8 0a 00 00 10   b       LAB_00087c04
00087bdc 21 80 40 00   _move   s0,v0
```

Láthatjuk, hogy bár mi vezéreljük a stack teljes tartalmát az S1 regiszter hibás értéket kapott, ezáltal nem tudtuk átvinni a PC (Program Counter) regiszter feletti irányítást, ami egy megoldandó probléma az exploit fejlesztéséhez, de a gyakorlat azt mutatja, hogy lehetséges :).

Összegezve tehát, van egy V14 hardware verziójú legújabb tl-wr841n routerünk, amin a legfrissebb firmware fut és van egy kihasználható LAN oldali sérülékenységekünk.

Ez nagyon jól hangzik viszont van egy kis gond. A vizsgált firmware nem a legfrissebb firmware volt! Pontosabban az volt, csak mégsem. Ez némi magyarázatra szorul igaz!?

Tehát amikor meglátogatjuk a tp-link hivatalos weboldalát, azonnal átirányít a régióknak megfelelő oldalra, ahol a legfrissebb firmware verzió a **TL-WR841N(EU)_V14_200903**.

TL-WR841N(EU)_V14_200903		Letöltés
Kiadás dátuma: 2020-11-27	Nyelv: Angol	Fájl méret: 4.27 MB
Modifications and Bug Fixes:		
1. Enhanced safety		
2. Added the Led Control function		
3. Added the WAN Link Status function		
4. Optimized the wireless function		
5. Optimized user experience of configuring the router		

De mi történik, ha maradunk az eredeti oldalon? Nos igen, itt egy jóval újabb firmware-t találunk a TL-WR841N(US)_V14_220121.

TL-WR841N(US)_V14_220121		Download
Published Date: 2022-03-11	Language: English	File Size: 4.34 MB

Release note:
Modifications and Bug Fixes:
Enhance device security.

Viszont, amikor le akarjuk tölteni az itt elérhető legfrissebb firmware-t az oldal üzen nekünk, hogy arra mindenképpen figyeljünk, hogy a vásárlás helyének megfelelő hivatalos weboldalról töltsük le a frissítést.

TL-WR841N(US)_V14_220121

Important Notice

Please upgrade firmware/software from the local TP-Link official website of the purchase location for your TP-Link device, otherwise it may cause upgrade failure or mistakes and be against the warranty.

Still DownloadGo to Local Website

Erre egyébként a magyar weboldal is felhívja a figyelmet. Az EU és US firmware-ek eltérnek egymástól és a helytelen firmware frissítés károsíthatja a készüléket és egyébként még ha nem is, a garanciát mindenképpen elveszítjük.

Frissítés

FONTOS: A frissítéskor legyen körültekintő, hogy elkerülje a készülék használhatatlanná válását, és kövesse az alábbi útmutatót a helyes frissítési folyamathoz:

Kérjük, ellenőrizze a készülék hardver verzióját a megfelelő firmware verzió eléréséhez. A helytelen firmware frissítés károsíthatja a készüléket, és érvényteleníti a garanciát. (Általában v1.x = V1);

Nem ajánlatos ezzel a firmware-rel frissíteni olyan készülékezt, aminek régió megjelölése eltérő. Kérjük, keresse ki [itt](#) az ön régióját a legmegfelelőbb firmware kiválasztásához. (Pl.: az EU és a US megjelölésű firmware-ek eltérnek egymástól)

Most ott tartunk, hogy van egy legfrissebb EU firmware-ünk ami sérülékeny és van egy némileg frissebb US verziójú firmware amire a gyártó szerint nem szabad frissíteni, de legalábbis mindenképpen kockázatos! Mivel nem tudjuk, hogy a legfrissebb US firmware a sérülékenységekben érintett-e, úgy döntöttünk, hogy megvizsgáljuk mielőtt megkíséreljük a frissítést az US verzióval.

TL-WR841N(EU)_V14_200903

```
66     }
67     if (pcVar3 == (char *)0x0) {
68         bVar1 = true;
69         strcpy(local_549 + 1,pcVar4 + 1);
70     }
71     else {
72         strncpy(local_549 + 1,pcVar4 + 1,(size_t)(pcVar3 + (-1 - (int)pcVar4)));
73         local_549[(int)(pcVar3 + (-1 - (int)pcVar4) + 1)] = '\0';
74         param_4 = pcVar3 + 1;
75         if (pcVar3[1] == '\0') {
76             bVar1 = true;
77             pcVar3 = (char *)0x0;
78         }
79         else {
80             pcVar3 = strchr(param_4,10);
81         }
82     }
```

TL-WR841N(US)_V14_220121

```
72     }
73     if (pcVar3 == (char *)0x0) {
74         local_2c = pcVar4 + 1;
75         sVar6 = strlen(pcVar4 + 1);
76         if (0x513 < sVar6) {
77             uVar8 = 0x7ed;
78             goto LAB_00088e14;
79         }
80         bVar1 = true;
81         strcpy(local_545 + 1,local_2c);
82     }
83     else {
84         pcVar7 = pcVar3 + -(int)pcVar4;
85         if (0x514 < (int)pcVar7) {
86             uVar8 = 0x7d7;
87 LAB_00088e14:
88             cdbg_printf(8,"dm_fillObjByStr",uVar8,"Parameter invalid");
89             return 0x232f;
90         }
91         strncpy(local_545 + 1,pcVar4 + 1,(size_t)(pcVar7 + -1));
92         local_545[(int)(pcVar7 + -1 + 1)] = '\0';
93         param_4 = pcVar3 + 1;
94         if (pcVar3[1] == '\0') {
95             bVar1 = true;
96             pcVar3 = (char *)0x0;
97         }
98         else {
99             pcVar3 = strchr(param_4,10);
100     }
```

Ha összehasonlítjuk a két firmware-t láthatjuk, hogy a US verzióban javítva van a hiba és így a sérülékenység nem kihasználható. Ez nagyszerű hiszen van olyan firmware amivel ha tudjuk frissíteni az eszközt, megszünteti a sérülékenységet.

SPOILER, nem fogunk tudni frissíteni. Amint a képen is látható, ha megpróbáljunk az US verziójú firmware-el frissíteni a routert, hibaüzenetet kapunk.

TP-Link Wireless N Router WR841N
Model No. TL-WR841N

Firmware Upgrade

Firmware File Path:

Tallózás...

TL-WR841Nv14_US_0.9.1_4.19_up_boot[220121-rel58074].bin

Firmware version:

0.9.1 4.17 v0001.0 Build 200903 Rel.58674n

Hardware version:

TL-WR841N v14 00000014

Upgrade

TP-Link Wireless N Router WR841N
Model No. TL-WR841N

Error

Error code: 4503

The uploaded file was not accepted by the device.

Back

Újra összefoglalva az egészet. A tp-link **TL-WR841N V14 EU** router legfrissebb firmware verziója autentikáció utáni távoli kód futtatás sérülékenységben érintett. Az EU firmware legutolsó elérhető verzióját 2020 11 27-én adták ki. Ezzel szemben a TL-WR841N V14 US routerek esetében elérhető egy sokkal újabb firmware (2022 03 11), amiben javítva van a sérülékenység, ezt viszont nem tudjuk telepíteni az EU verziójú routerünkre.

Az egész egyébként rendkívül érdekes olyan tekintetben, hogy úgy tűnik a gyártó tisztában volt a sérülékenységgel, hiszen a US verzióban elérhető a javítás, viszont az EU routerekhez mégsem tette elérhetővé a javított firmware képet.