Re: TP-LINK Cloud Cameras NCXXX Remote NULL Pointer Dereference

From: Pietro Oliva <pietroliva () gmail com>
Date: Thu, 9 Apr 2020 17:32:14 +0100

```
[UPDATE 08/04/2020] - The vendor has published firmware updates to fix
the issue.

Vulnerability title: TP-LINK Cloud Cameras NCXXX Remote NULL Pointer Dereference
Author: Pietro Oliva
CVE: CVE-2020-10231
Vendor: TP-LINK
Product: NC200, NC210, NC220, NC230, NC250, NC260, NC450
Affected version: NC200 <= 2.1.8 build 171109, NC210 <= 1.0.9 build 171214,
                            NC220 <= 1.3.0 build 180105, NC230 <=
1.3.0 build 171205,
                            NC250 <= 1.3.0 build 171205, NC260 <=
1.5.1 build 190805,
                            NC450 <= 1.5.0 build 181022
Fixed in 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

Description:
The issue is located in the httpLoginRpm method of the ipcamera binary (handler
method for /login.fcgi), where after successful login, there is no check for
NULL in the return value of httpGetEnv(environment, "HTTP_USER_AGENT"). Shortly
after that, there is a call to strstr(user_agent_string, "Firefox") and if a
User-Agent header is not specified by the client, httpGetEnv will return NULL,
and a NULL pointer dereference occurs when calling strstr, with consequent crash
of the ipcamera process.

Impact:
After the crash, the web interface on port 80 will not be available anymore.

Exploitation:
An attacker could exploit this issue by just sending a login request with valid
credentials (such as admin or limited user), but without an user-agent HTTP
header. Default credentials can be used to bypass the credentials requirement.

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

0x0047dca0   lw a0, (user_arg)
0x0047dca4   lw a1, (password_arg)
0x0047dca8   lw t9, -sym.swUMMatchPassword(gp)
0x0047dcac   nop
0x0047dcb0   jalr t9
0x0047dcb4   nop
0x0047dcb8   lw gp, (saved_gp)
0x0047dcbc   sw v0, (auth_result)
0x0047dcc0   lw v0, (auth_result)
0x0047dcc4   nop
0x0047dcc8   bnez v0, 0x47de34
0x0047dccc   nop
0x0047dcd0   sw zero, (arg_54h)
0x0047dcd4   lw a0, (environment)
0x0047dcd8   lw a1, -0x7fe4(gp)
0x0047dcdc   nop
0x0047dce0   addiu a1, a1, -0x7cb0       ; "HTTP_USER_AGENT"
0x0047dce4   lw t9, -sym.httpGetEnv(gp)
0x0047dce8   nop
0x0047dcec   jalr t9
0x0047dcf0   nop
0x0047dcf4   lw gp, (saved_gp)
0x0047dcf8   sw v0, (user_agent_ptr)
0x0047dcfc   lw a0, (user_agent_ptr)     ; <== This pointer could be NULL
0x0047dd00   lw a1, -0x7fe4(gp)
0x0047dd04   nop
0x0047dd08   addiu a1, a1, -0x7ca0       ; "Firefox"
0x0047dd0c   lw t9, -sym.imp.strstr(gp)
0x0047dd10   nop
0x0047dd14   jalr t9

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:

2nd December 2019 - Initial vulnerability report for NC200.

4th December 2019 - Vendor confirms vulnerablity but does not start fixing
                                  due to the product being end-of-life.

4th December 2019 - Notified vendor the vulnerability details will be public
                                  and it should be fixed.

6th December 2019 - Thanks for your opinion, we will discuss and write back
                                  to you.

<silence>

7th February 2020 - Notified vendor issue exists on NC450 and possibly all
                                 models in between. Fixed a disclosure
deadline in 30 days.

8th February 2020 - Vendor: We will check but please be patient.

18th February 2020 - We failed to reproduce the issue with the provided PoC.

<trying to troubleshoot>

24th February 2020 - Reverse engineered all the firmware images on behalf of
                                  the vendor and notified they were
all vulnerable.

2nd March 2020 - Vendor asks to check fixes for NC200.
```

2nd March 2020 - Confirmed fix. Asked the vendor to do the same on all cameras.

3rd March 2020 - Vendor will check on other cameras, but will take some time.

3rd March 2020 - Asked the vendor to be quick.

9th March 2020 - Notified CVE identifier to vendor, gave extra week to patch.

9th March 2020 - Vendor is testing fix on all models.

13th March 2020 - Vendor asks to confirm fixes.

13th March 2020 - Confirmed fixes and asked the vendor to publish updates.
                  Disclosure delayed one week to give some time to patch if
                  the vendor published firmware updates.

29th March 2020 - No updates have been made public by the vendor. Releasing
                  details to the public after almost 4 months from initial notification.

08 April 2020 - Firmware updates fixing the vulnerability released by the vendor.

09 April 2020 - Updated this vulnerability disclosure with fix information.

Il giorno dom 29 mar 2020 alle ore 20:47 Pietro Oliva
<pietroliva () gmail com> ha scritto:

> Vulnerability title: TP-LINK Cloud Cameras NCXXX Remote NULL Pointer Dereference
> Author: Pietro Oliva
> CVE: CVE-2020-10231
> Vendor: TP-LINK
> Product: NC200, NC210, NC220, NC230, NC250, NC260, NC450
> Affected version: NC200 <= 2.1.8 build 171109, NC210 <= 1.0.9 build 171214,
>   NC220 <= 1.3.0 build 180105, NC230 <= 1.3.0 build 171205,
>   NC250 <= 1.3.0 build 171205, NC260 <= 1.5.1 build 190805,
>   NC450 <= 1.5.0 build 181022
>
> Description:
> The issue is located in the httpLoginRpm method of the ipcamera binary (handler
> method for /login.fcgi), where after successful login, there is no check for
> NULL in the return value of httpGetEnv(environment, "HTTP_USER_AGENT"). Shortly
> after that, there is a call to strstr(user_agent_string, "Firefox") and if a
> User-Agent header is not specified by the client, httpGetEnv will return NULL,
> and a NULL pointer dereference occurs when calling strstr, with consequent crash
> of the ipcamera process.
>
> Impact:
> After the crash, the web interface on port 80 will not be available anymore.
>
> Exploitation:
> An attacker could exploit this issue by just sending a login request with valid
> credentials (such as admin or limited user), but without an user-agent HTTP
> header. Default credentials can be used to bypass the credentials requirement.
>
> Evidence:
> The disassembly of affected code from an NC200 camera is shown below:
>
> ```
> 0x0047dca0   lw a0, (user_arg)
> 0x0047dca4   lw a1, (password_arg)
> 0x0047dca8   lw t9, -sym.swUMMatchPassword(gp)
> 0x0047dcac   nop
> 0x0047dcb0   jalr t9
> 0x0047dcb4   nop
> 0x0047dcb8   lw gp, (saved_gp)
> 0x0047dcbc   sw v0, (auth_result)
> 0x0047dcc0   lw v0, (auth_result)
> 0x0047dcc4   nop
> 0x0047dcc8   bnez v0, 0x47de34
> 0x0047dccc   nop
> 0x0047dcd0   sw zero, (arg_54h)
> 0x0047dcd4   lw a0, (environment)
> 0x0047dcd8   lw a1, -0x7fe4(gp)
> 0x0047dcdc   nop
> 0x0047dce0   addiu a1, a1, -0x7cb0       ; "HTTP_USER_AGENT"
> 0x0047dce4   lw t9, -sym.httpGetEnv(gp)
> 0x0047dce8   nop
> 0x0047dcec   jalr t9
> 0x0047dcf0   nop
> 0x0047dcf4   lw gp, (saved_gp)
> 0x0047dcf8   sw v0, (user_agent_ptr)
> 0x0047dcfc   lw a0, (user_agent_ptr)     ; <== This pointer could be NULL
> 0x0047dd00   lw a1, -0x7fe4(gp)
> 0x0047dd04   nop
> 0x0047dd08   addiu a1, a1, -0x7ca0       ; "Firefox"
> 0x0047dd0c   lw t9, -sym.imp.strstr(gp)
> 0x0047dd10   nop
> 0x0047dd14   jalr t9
> ```
>
> Disclosure timeline:
>
> 2nd December 2019 - Initial vulnerability report for NC200.
>
> 4th December 2019 - Vendor confirms vulnerablity but does not start fixing
>   due to the product being end-of-life.
>
> 4th December 2019 - Notified vendor the vulnerability details will be public
>   and it should be fixed.
>
> 6th December 2019 - Thanks for your opinion, we will discuss and write back
>   to you.
>
> <silence>
>
> 7th February 2020 - Notified vendor issue exists on NC450 and possibly all
>   models in between. Fixed a disclosure deadline in 30 days.
>
> 8th February 2020 - Vendor: We will check but please be patient.
>
> 18th February 2020 - We failed to reproduce the issue with the provided PoC.
>
> <trying to troubleshoot>
>
> 24th February 2020 - Reverse engineered all the firmware images on behalf of
>   the vendor and notified they were all vulnerable.
>
> 2nd March 2020 - Vendor asks to check fixes for NC200.
>
> 2nd March 2020 - Confirmed fix. Asked the vendor to do the same on all cameras.
>
> 3rd March 2020 - Vendor will check on other cameras, but will take some time.
>
> 3rd March 2020 - Asked the vendor to be quick.
>
> 9th March 2020 - Notified CVE identifier to vendor, gave extra week to patch.
>
> 9th March 2020 - Vendor is testing fix on all models.
>
> 13th March 2020 - Vendor asks to confirm fixes.
>
> 13th March 2020 - Confirmed fixes and asked the vendor to publish updates.
>   Disclosure delayed one week to give some time to patch if
>   the vendor published firmware updates.
>
> 29th March 2020 - No updates have been made public by the vendor. Releasing

> details to the public after almost 4 months from initial notification.

Current thread:

Re: TP-LINK Cloud Cameras NCXXX Remote NULL Pointer Dereference ***Pietro Oliva (Apr 10)***