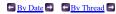


Full Disclosure mailing list archives





List Archive Search

TP-LINK Cloud Cameras NCXXX Remote NULL Pointer Dereference

From: Pietro Oliva <pietroliva () gmail com> Date: Sun, 29 Mar 2020 20:47:15 +0100

```
Vulnerability title: TP-LINK Cloud Cameras NCXXX Remote NULL Pointer Dereference
Vulnerability title: if January Carlo 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:

```
lw a0, (user_arg)
lw a1, (password_arg)
lw t9, -sym.swUMMatchPassword(gp)
0x0047dca0
0x0047dca4
0x0047dca4
0x0047dca5
0x0047dcb4
0x0047dcb4
0x0047dcb4
0x0047dcb4
0x0047dcb5
0x0047dcb6
0x0047dccd
0x0047dccd
0x0047dccd
0x0047dccd
0x0047dcdd
                                nop
jalr t9
                                nop
lw gp, (saved_gp)
sw v0, (auth_result)
lw v0, (auth_result)
                                  nop
bnez v0, 0x47de34
                                nop
sw zero, (arg_54h)
lw a0, (environment
lw a1, -0x7fe4(gp)
                                 nop nop addiu al, al, -0x7cb0 ; "HTTP_USER_AGENT" lw t9, -sym.httpGetEnv(gp)
                                lw tt, -sym.ntrpoetEliv(g
nop
jalr t9
nop
lw gp, (saved_gp)
sw v0, (user_agent_ptr)
lw a1, -0x7fe4(gp)
                                                                                                         ; <== This pointer could be NULL
 0x0047dd00
                                nop addiu al, al, -0x7ca0 ; "Firefox" lw t9, -sym.imp.strstr(gp)
 0x0047dd04
 0x0047dd08
 0x0047dd0c
0x0047dd10 nop
0x0047dd14 jalr t9
 0x0047dd10
```

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.

By Date By Thread

Current thread:

TP-LINK Cloud Cameras NCXXX Remote NULL Pointer Dereference Pietro Oliva (Mar 31)

Site Search						
Nmap Security Scanner	Npcap packet	Security Lists	Security Tools	About		
	capture	Nmap Announce	Vuln scanners	About/Contact		
Ref Guide	User's Guide	Nmap Dev	Password audit	Privacy		
Install Guide	API docs	Full Disclosure	Web scanners	Advertising		
Docs	Download	Open Source Security	Wireless	Nmap Public Source		
Download	Npcap OEM	BreachExchange	Exploitation	License		
Nmap OEM		DieachExchange	Exploitation			