

TP-LINK Cloud Cameras NCXXX Remote NULL Pointer Dereference

Authored by [Pietro Oliva](#)

Posted [Apr 1, 2020](#)

TP-LINK cloud cameras including products NC200, NC210, NC220, NC230, NC250, NC260, and NC450 suffer from a remote null pointer dereference vulnerability.

tags | [advisory](#) | [remote](#)

advisories | [CVE-2020-10231](#)

SHA-256 | [9fd1d7280c6b43c3460d7edc998309cea3240cebfc388e46f582ecf935c7deb71](#) [Download](#) | [Favorite](#) | [View](#)

Related Files

Share This

Like

Twitter

LinkedIn

Reddit

Digg

StumbleUpon

[Change Mirror](#)[Download](#)

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.swDMatchPassword(gp)
0x0047dcac  nop
0x0047dcb0  jalr t9
0x0047dcb4  nop
0x0047dcb8  lw gp, (saved_gp)
0x0047dcbc  sw v0, (auth_result)
0x0047dccc  lw v0, (auth_result)
0x0047dcd0  nop
0x0047dcd4  bnez v0, 0x47de34
0x0047dcd8  nop
0x0047dcdc  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 vulnerability 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.

Search ...

 Follow us on Twitter

 Subscribe to an RSS Feed

File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr
Sa					
				1	2
3					
4	5	6	7	8	9
10					
11	12	13	14	15	16
17					
18	19	20	21	22	23
24					
25	26	27	28	29	30
31					

Top Authors In Last 30 Days

Red Hat 154 files
Ubuntu 73 files
LiquidWorm 23 files
Debian 18 files
malvuln 11 files
nu11security 11 files
Gentoo 9 files
Google Security Research 8 files
T. Weber 4 files
Julien Ahrens 4 files

File Tags

ActiveX (932)	December 2022
Advisory (79,754)	November 2022
Arbitrary (15,694)	October 2022
BBS (2,859)	September 2022
Bypass (1,619)	August 2022
CGI (1,018)	July 2022
Code Execution (8,926)	June 2022
Conference (673)	May 2022
Cracker (840)	April 2022
CSRF (3,290)	March 2022
DoS (22,602)	February 2022
Encryption (2,349)	January 2022
Exploit (50,359)	Older
File Inclusion (4,165)	

File Archives

File Upload (946)

Firewall (821)	AIX (426)
Info Disclosure (2,660)	Apple (1,926)
Intrusion Detection (867)	BSD (370)
Java (2,899)	CentOS (55)
JavaScript (821)	Cisco (1,917)
Kernel (6,291)	Debian (6,634)
Local (14,201)	Fedora (1,600)
Magazine (586)	FreeBSD (1,242)
Overflow (12,419)	Gentoo (4,272)
Perl (1,418)	HPUX (878)
PHP (5,093)	IOS (330)
Proof of Concept (2,291)	iPhone (108)
Protocol (3,435)	IRIX (220)
Python (1,467)	Juniper (67)
Remote (30,044)	Linux (44,315)
Root (3,504)	Mac OS X (684)
Ruby (594)	Mandriva (3,105)
Scanner (1,631)	NetBSD (255)
Security Tool (7,777)	OpenBSD (479)
Shell (3,103)	RedHat (12,469)
Shellcode (1,204)	Slackware (941)
Sniffer (886)	Solaris (1,607)

- Spoof (2,166)

SQL Injection (16,102)

TCP (2,379)

Trojan (686)

UDP (876)

Virus (662)

Vulnerability (31,136)

Web (9,365)

Whitepaper (3,729)

x86 (946)

XSS (17,494)

Other

SUSE (1,444)

Ubuntu (8,199)

UNIX (9,159)

UnixWare (185)

Windows (6,511)

Other

Site Links

- News by Month

News Tags

Files by Month

File Tags

File Directory

About Us

- History & Purpose

Contact Information

Terms of Service

Privacy Statement

Copyright Information

Hosting By

Rokasec



Follow us on Twitter



Subscribe to an RSS Feed