TP-LINK Cloud Cameras NCXXX Stack Overflow

Authored by Pietro Oliva

Posted Jun 16, 2020

TP-LINK Cloud Cameras NCXXX suffer from a DelMultiUser stack overflow vulnerability.

tags | exploit, overflow
advisories | CVE-2020-13224
SHA-256 | 8ceea48329dd3d48af63a7ccdec830b47ac2bcf4bf77d8735c577b80b70e19b4 **Download** | **Favorite** | **View**

Related Files

Change Mirror Download

```
Vulnerability title: TP-LINK Cloud Cameras NCXXX DelMultiUser Stack Overflow
Author: Pietro Oliva
CVE: CVE-2020-13224
Vendor: TP-LINK
Product: NC200, NC210, NC220, NC230, NC250, NC260, NC450
Affected versions: 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

Fixed versions:    NC200 <= 2.1.11 build 200508, NC210 <= 1.0.11 build 200612,
                   NC220 <= 1.3.2 build 200508, NC230 <= 1.3.2 build 200508,
                   NC250 <= 1.3.2 build 200508, NC260 <= 1.5.4 build_200508,
                   NC450 <= 1.5.5 build 200508

Description:
The issue is located in the httpDelMultiUserRpm method of the ipcamera binary
(Called when deleting multiple users via /delmultiuser.fcgi), where a
comma-delimited list of usernames is passed as an input, and a list of error
codes for each user deletion attempt is returned to the user via HTTP. The list
of error codes returned to the user is temporary stored in a fixed-size stack
buffer, while there in no limit on the number of usernames that the user can
specify. Since the error codes are concatenated in a loop without any boundary
checks until a string terminator has been found in the user-supplied string, a
stack-based buffer overflow can occur if the user provided an input string
with enough commas or usernames.

Impact:
Attackers could exploit this vulnerability to remotely crash the ipcamera
process, or remotely execute arbitrary code as root.

Exploitation:
An attacker would first need to authenticate to the web interface and make a
request similar to the following to trigger a crash of the ipcamera process:

POST /delmultiuser.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

Usernames=,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,&token=xxxxx"


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

sym.httpDelMultiUserRpm:

; Get pointer to Usernames param from HTTP request
    ||    0x0047ee90  lw a0, (env)
    ||    0x0047ee94  lw a1, -0x7fe4(gp)
    ||    0x0047ee98  nop
    ||    0x0047ee9c  addiu a1, a1, -0x73b0 ; "Usernames" string
    ||    0x0047eea0  lw t9, -sym.httpGetEnv(gp)
    ||    0x0047eea4  nop
    ||    0x0047eea8  jalr t9
    ||    0x0047eeac  nop

; Save the pointer and return error if it is NULL
    ||    0x0047eeb0  lw gp, (arg_10h)
    ||    0x0047eeb4  sw v0, (arg_usernames)
    ||    0x0047eeb8  lw v0, (arg_usernames)
    ||    0x0047eebc  nop
    ||┌─< 0x0047eec0  bnez v0, 0x47eed4
    |||   0x0047eec4  nop
    |||   0x0047eec8  addiu v0, zero, -1
   ┌────< 0x0047eecc  b 0x47f0bc
   ||||   0x0047eed0  sw v0, (arg_46ch)

; If the pointer is not null, initialize to 0 the error code buffer on the stack
   |||└─> 0x0047eed4  addiu v0, fp, 0x40
   |||    0x0047eed8  move a0, v0
   |||    0x0047eedc  move a1, zero
   |||    0x0047eee0  addiu a2, zero, 0x400
   |||    0x0047eee4  lw t9, -sym.imp.memset(gp)
   |||    0x0047eee8  nop
   |||    0x0047eeec  jalr t9
   |||    0x0047eef0  nop
   |||    0x0047eef4  lw gp, (arg_10h)

; Copy the arg_usernames pointer to arg_usernames_copy
   |||    0x0047eef8  lw v0, (arg_usernames)
   |||    0x0047eefc  nop
   |||    0x0047ef00  sw v0, (arg_usernames_copy)

; Get a pointer to the first occurrence of the comma character and store it
   |||┌─> 0x0047ef04  lw a0, (arg_usernames_copy)
   |||¦   0x0047ef08  addiu a1, zero, 0x2c
   |||¦   0x0047ef0c  lw t9, -sym.imp.strchr(gp)
   |||¦   0x0047ef10  nop
   |||¦   0x0047ef14  jalr t9
   |||¦   0x0047ef18  nop
   |||¦   0x0047ef1c  lw gp, (arg_10h)
   |||¦   0x0047ef20  sw v0, (ptr_to_next_comma)

; If the pointer is NULL go and delete the last username in the list
   |||¦   0x0047ef24  lw v0, (ptr_to_next_comma)
   |||¦   0x0047ef28  nop
  ┌─────< 0x0047ef2c  beqz v0, 0x47efc0
  ||||¦   0x0047ef30  nop

; Replace the comma character with a string terminator and delete the user
  ||||¦   0x0047ef34  lw v0, (ptr_to_next_comma)
  ||||¦   0x0047ef38  nop
  ||||¦   0x0047ef3c  sb zero, (v0)
  ||||¦   0x0047ef40  lw a0, (arg_usernames_copy)
  ||||¦   0x0047ef44  lw t9, -sym.swUMDelUser(gp)
  ||||¦   0x0047ef48  nop
  ||||¦   0x0047ef4c  jalr t9
  ||||¦   0x0047ef50  nop

; Create a string with the error code from swUMDelUser
  ||||¦   0x0047ef54  lw gp, (arg_10h)
  ||||¦   0x0047ef58  sw v0, (deluser_error_code)
  ||||¦   0x0047ef5c  addiu v0, fp, 0x448
  ||||¦   0x0047ef60  move a0, v0
  ||||¦   0x0047ef64  lw a1, -0x7fe4(gp)
```

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
nu11secur1ty 11 files
Gentoo 9 files
Google Security Research 8 files
T. Weber 4 files
Julien Ahrens 4 files

File Tags

ActiveX (932)
Advisory (79,754)
Arbitrary (15,694)
BBS (2,859)
Bypass (1,619)
CGI (1,018)
Code Execution (6,926)
Conference (673)
Cracker (840)
CSRF (3,290)
DoS (22,602)
Encryption (2,349)
Exploit (50,359)
File Inclusion (4,165)
File Upload (946)
Firewall (821)
Info Disclosure (2,660)
Intrusion Detection (867)
Java (2,899)
JavaScript (821)
Kernel (6,291)
Local (14,201)
Magazine (586)
Overflow (12,419)
Perl (1,418)
PHP (5,093)
Proof of Concept (2,291)
Protocol (3,435)
Python (1,467)
Remote (30,044)
Root (3,504)
Ruby (594)
Scanner (1,631)
Security Tool (7,777)
Shell (3,103)
Shellcode (1,204)
Sniffer (886)

File Archives

December 2022
November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
Older

Systems

AIX (426)
Apple (1,926)
BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,634)
Fedora (1,690)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
iOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,315)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,469)
Slackware (941)
Solaris (1,607)

```
 |||||   0x0047ef68  nop
 |||||   0x0047ef6c  addiu a1, a1, -0x73a4       ; '{"errorCode":&d},'
 |||||   0x0047ef70  lw a2, (deluser_error_code)
 |||||   0x0047ef74  lw t9, -sym.imp.sprintf(gp)
 |||||   0x0047ef78  nop
 |||||   0x0047ef7c  jalr t9
 |||||   0x0047ef80  nop

; Concatenate the error code string with other error codes on the stack
 |||||   0x0047ef84  lw gp, (arg_10h)
 |||||   0x0047ef88  addiu v0, fp, 0x40
 |||||   0x0047ef8c  addiu v1, fp, 0x448
 |||||   0x0047ef90  move a0, v0
 |||||   0x0047ef94  move a1, v1
 |||||   0x0047ef98  lw t9, -sym.imp.strcat(gp) ; concatenate err code
 |||||   0x0047ef9c  nop
 |||||   0x0047efa0  jalr t9
 |||||   0x0047efa4  nop

; Increase the pointer by one to the next username
 |||||   0x0047efa8  lw gp, (arg_10h)
 |||||   0x0047efac  lw v0, (ptr_to_next_comma)
 |||||   0x0047efb0  nop
 |||||   0x0047efb4  addiu v0, v0, 1

; Store the updated pointer and skip the last/only username deletion code
 ,=====< 0x0047efb8  b 0x47f034
 |||||   0x0047efbc  sw v0, (arg_usernames_copy)

; Delete the last/only username in the list and concatenate error code
 |`----> 0x0047efc0  lw a0, (arg_usernames_copy)
 | |||   0x0047efc4  lw t9, -sym.swUMDelUser(gp)
 | |||   0x0047efc8  nop
 | |||   0x0047efcc  jalr t9
 | |||   0x0047efd0  nop
 | |||   0x0047efd4  lw gp, (arg_10h)
 | |||   0x0047efd8  sw v0, (deluser_error_code)
 | |||   0x0047efdc  addiu v0, fp, 0x448
 | |||   0x0047efe0  move a0, v0
 | |||   0x0047efe4  lw a1, -0x7fe4(gp)
 | |||   0x0047efe8  nop
 | |||   0x0047efec  addiu a1, a1, -0x73a4      ; '{"errorCode":&d},'
 | |||   0x0047eff0  lw a2, (deluser_error_code)
 | |||   0x0047eff4  lw t9, -sym.imp.sprintf(gp)
 | |||   0x0047eff8  nop
 | |||   0x0047effc  jalr t9
 | |||   0x0047f000  nop
 | |||   0x0047f004  lw gp, (arg_10h)
 | |||   0x0047f008  addiu v0, fp, 0x40
 | |||   0x0047f00c  addiu v1, fp, 0x448
 | |||   0x0047f010  move a0, v0
 | |||   0x0047f014  move a1, v1
 | |||   0x0047f018  lw t9, -sym.imp.strcat(gp) ; Concatenate err code
 | |||   0x0047f01c  nop
 | |||   0x0047f020  jalr t9
 | |||   0x0047f024  nop
 | |||   0x0047f028  lw gp, (arg_10h)
 | ,=====< 0x0047f02c  b 0x47f04c
 |||||   0x0047f030  nop

; Checks if the string terminator has been found.
 `-----> 0x0047f034  lw v0, (ptr_to_next_comma)
  ||||   0x0047f038  nop

; If yes, return the error codes to the user via HTTP
 ,=====< 0x0047f03c  beqz v0, 0x47f04c

; Otherwise, continue deleting users until the NULL terminator is found.
 |||||   0x0047f040  nop
 |||||`-< 0x0047f044  b 0x47ef04


Mitigating factors:
There is very limited control over the buffer that will eventually overwrite
the saved return address. The only part of the buffer that can be slightly
controlled is the error code by using existing, non-existing, or invalid
usernames, since error codes can change in content and length. If an attacker
managed to find a way to carefully combine error codes and obtain a valid
address after return address overwrite, arbitrary code execution as root
could be achieved.

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 May 2020 - Vulnerability reported to vendor.
19th May 2020 - Patched firmware provided by vendor for verification.
19th May 2020 - Confirmed the vulnerability was fixed.
15th June 2020 - Firmware updates released to the public.
15th June 2020 - Vulnerability details are made public.
```