TP-LINK Cloud Cameras NCXXX SetEncryptKey Command Injection

Authored by Pietro Oliva

Posted May 1, 2020

TP-LINK Cloud Cameras including products NC260 and NC450 suffer from a command injection vulnerability. The issue is located in the httpSetEncryptKeyRpm method (handler for /setEncryptKey.fcgi) of the ipcamera binary, where the user-controlled EncryptKey parameter is used directly as part of a command line to be executed as root without any input sanitization.

tags | exploit, root
advisories | CVE-2020-12111
SHA-256 | 7c6daeba86b10ee66abb00c8b005635251b71f86700d9246cd9f53c346cb9ee0

Download | Favorite | View

Related Files

Change Mirror Download

```
Vulnerability title: TP-LINK Cloud Cameras NCXXX SetEncryptKey Command Injection
Author: Pietro Oliva
CVE: CVE-2020-12111
Vendor: TP-LINK
Product: NC260, NC450
Affected version: NC260 <= 1.5.2 build 200304, NC450 <= 1.5.3 build 200304
Fixed version:    NC260 <= 1.5.3 build_200401, NC450 <= 1.5.4 build 200401

Description:
The issue is located in the httpSetEncryptKeyRpm method (handler for
/setEncryptKey.fcgi) of the ipcamera binary, where the user-controlled
EncryptKey parameter is used directly as part of a command line to be executed
as root without any input sanitization.

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
POST request to /setEncryptKey.fcgi. Commands to be executed with root
privileges can be injected in the EncryptKey parameter.

Evidence:
The disassembly of affected code from an NC450 camera is shown below:

httpSetEncryptKeyRpm:

0x00491728   lw a0, -0x7fd4(gp)
0x0049172c   nop
0x00491730   addiu a0, a0, 0x3344        ; "echo %s > %s/%08X"
0x00491734   lw a1, (EncryptKey_param)   ; Attacker controlled string
0x00491738   lw a2, -0x7fd4(gp)
0x0049173c   nop
0x00491740   addiu a2, a2, 0x3330        ; 0x583330 ; "/tmp/.encryptkey/"
0x00491744   lw a3, -0x7fe8(gp)
0x00491748   nop
0x0049174c   addiu a3, a3, -0xf10
0x00491750   lw a3, (a3)
0x00491754   lw t9, -sym.cmCommand(gp)
0x00491758   nop
0x0049175c   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:
29th March 2020 - Vulnerability reported to vendor.
27th April 2020 - Patched firmware provided by vendor for verification.
27th April 2020 - Confirmed the vulnerability was fixed.
29th April 2020 - Firmware updates released to the public.
29th April 2020 - Vulnerability details are made public.
```

Login or Register to add favorites

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)

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