



Site Search



[Full Disclosure](#) mailing list archives



[By Date](#) [By Thread](#)

List Archive Search



TP-LINK Cloud Cameras NCXXX SetEncryptKey Command Injection

From: Pietro Oliva <pietroliva () gmail com>

Date: Wed, 29 Apr 2020 23:47:12 +0100

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/nc240/#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.

Sent through the Full Disclosure mailing list
<https://nmap.org/mailman/listinfo/fulldisclosure>
Web Archives & RSS: <http://seclists.org/fulldisclosure/>

[By Date](#) [By Thread](#)

Current thread:

TP-LINK Cloud Cameras NCXXX SetEncryptKey Command Injection *Pietro Oliva (May 01)*

Site Search



Nmap Security Scanner

Ref Guide

Install Guide

Docs

Download

Nmap OEM

Npcap packet capture

User's Guide

API docs

Download

Npcap OEM

Security Lists

Nmap Announce

Nmap Dev

Full Disclosure

Open Source Security

BreachExchange

Security Tools

Vuln scanners

Password audit

Web scanners

Wireless

Exploitation

About

About/Contact

Privacy

Advertising

Nmap Public Source License

