TP-LINK Cloud Cameras NCXXX Hardcoded Encryption Key

Authored by Pietro Oliva

Posted May 1, 2020

TP-LINK Cloud Cameras including products NC200, NC210, NC220, NC230, NC250, NC260, and NC450 suffer from having a hardcoded encryption key. The issue is located in the methods swSystemBackup and sym.swSystemRestoreFile, where a hardcoded encryption key is used in order to encrypt/decrypt a config backup file. The algorithm in use is DES ECB with modified s-boxes and permutation tables.

tags | exploit
advisories | CVE-2020-12110
SHA-256 | 8a9bf019904b9da201926fdb2f4eca44ec5bb26ff30a3e12709465ed196958ca **Download** | **Favorite** | **View**

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
Vulnerability title: TP-LINK Cloud Cameras NCXXX Hardcoded Encryption Key
Author: Pietro Oliva
CVE: CVE-2020-12110
Vendor: TP-LINK
Product: NC200, NC210, NC220, NC230, NC250, NC260, NC450
Affected version: NC200 <= 2.1.9 build 200225, NC210 <= 1.0.9 build 200304,
                  NC220 <= 1.3.0 build 200304, NC230 <= 1.3.0 build 200304,
                  NC250 <= 1.3.0 build 200304, NC260 <= 1.5.2 build 200304,
                  NC450 <= 1.5.3 build 200304.

Fixed version:    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


Description:
The issue is located in the methods swSystemBackup and sym.swSystemRestoreFile,
where a hardcoded encryption key is used in order to encrypt/decrypt a config
backup file. The algorithm in use is DES ECB with modified s-boxes and
permutation tables.

Impact:
Attackers could exploit this vulnerability to decrypt backup files and get
access to sensitive data, such as the following:
-Alarm FTP server user and password
-Wlan passphrase
-PPPOE user and password
-Alarm SMTP server user and password
-DDNS user and password

In addition to that, attackers could forge an encrypted backup file that can
be restored via the web interface. This allowed arbitrary files to be written or
overwritten with arbitrary attacker-controlled contents. Needless to say, this
could result in permanent damage or code execution as root.

Exploitation:
An attacker would have to figure out the modified DES algorithm in order to be
able to encrypt/decrypt config backup files. This is not hard to do with some
google search. Once that has been done, attackers can either decrypt backup
files or create their own with custom contents, effectlively writing arbitrary
files on the device.


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

swSystemRestoreFile:

0x004a0f88   lui gp, 0xa
0x004a0f8c   addiu gp, gp, -0x5c78
0x004a0f90   addu gp, gp, t9
0x004a0f94   addiu sp, sp, -0x4f8
0x004a0f98   sw ra, (var_4f4h)
0x004a0f9c   sw fp, (var_4f0h)
0x004a0fa0   move fp, sp
0x004a0fa4   sw gp, (var_18h)
0x004a0fa8   sw a0, (encrypted_filename_ptr)
0x004a0fac   lw v0, -0x7fe4(gp)
0x004a0fb0   nop
0x004a0fb4   addiu v0, v0, -0x4c40       ; "/tmp/plainBackup"
0x004a0fb8   nop
0x004a0fbc   sw v0, (decrypted_filename_ptr)
0x004a0fc0   lw a0, (encrypted_filename_ptr)
0x004a0fc4   lw a1, -0x7fe4(gp)
0x004a0fc8   nop
0x004a0fcc   addiu a1, a1, -0x4c2c       ; "tp-link"
0x004a0fd0   lw a2, (decrypted_filename_ptr)
0x004a0fd4   lw t9, -sym.DES_Decrypt(gp)
0x004a0fd8   nop
0x004a0fdc   jalr t9

swSystemBackup:

0x004a1c54   lw a0, -0x7fe4(gp)
0x004a1c58   nop
0x004a1c5c   addiu a0, a0, -0x4bbc       ; "/usr/local/config/ipcamera/pBackup"
0x004a1c60   lw a1, -0x7fe4(gp)
0x004a1c64   nop
0x004a1c68   addiu a1, a1, -0x4c2c       ; "tp-link"
0x004a1c6c   lw a2, -0x7fe4(gp)
0x004a1c70   nop
0x004a1c74   addiu a2, a2, -0x4b84       ; "/usr/local/config/ipcamera/eBackup"
0x004a1c78   lw t9, -sym.DES_Encrypt(gp)
0x004a1c7c   nop
0x004a1c80   jalr t9

Mitigating factors:
-Almost every camera model has a different hardcoded key. However, this is not
hard to find and all cameras of the same model share the same encryption key
which cannot be changed.

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.
10th April 2020 - Patched firmware provided by vendor for verification.
10th April 2020 - Confirmed the vulnerability was fixed.
29th April 2020 - Firmware updates released to the public.
29th April 2020 - Vulnerability details are made public.
```

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

Author	Files
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

Tag	Count
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

System	Count
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)

Login or Register to add favorites

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