

« Sécurité » des objets connectés

Exemple de vulnérabilité

« Sécurité » des objets connectés

Découverte

```
nmap -T4 -F 134.206.NNN.MMM
```

```
Nmap scan report for xxxxx-clim.univ-lille1.fr
```

```
[...]
```

PORT	STATE	SERVICE
21/tcp	open	ftp
23/tcp	open	telnet
25/tcp	filtered	smtp
80/tcp	open	http

```
telnet xxxxx-clim.univ-lille1.fr
```

```
Trying 134.206.NNN.MMM...
```

```
Connected to xxxxx-clim.univ-lille1.fr.
```

```
Escape character is '^['.
```

```
Linux 2.4.21-rmk1 (pCOWeb) (ttya0)
```

« Sécurité » des objets connectés

Apprentissage

Google « pcoweb » :

➤ pCOWeb est une carte série Ethernet pour système pCO CAREL. Complètement personnalisable, elle permet d'accéder à toutes les variables **R/W** de l'automate et de facilement **modifier** certains paramètres utilisateurs comme par exemple un point de consigne

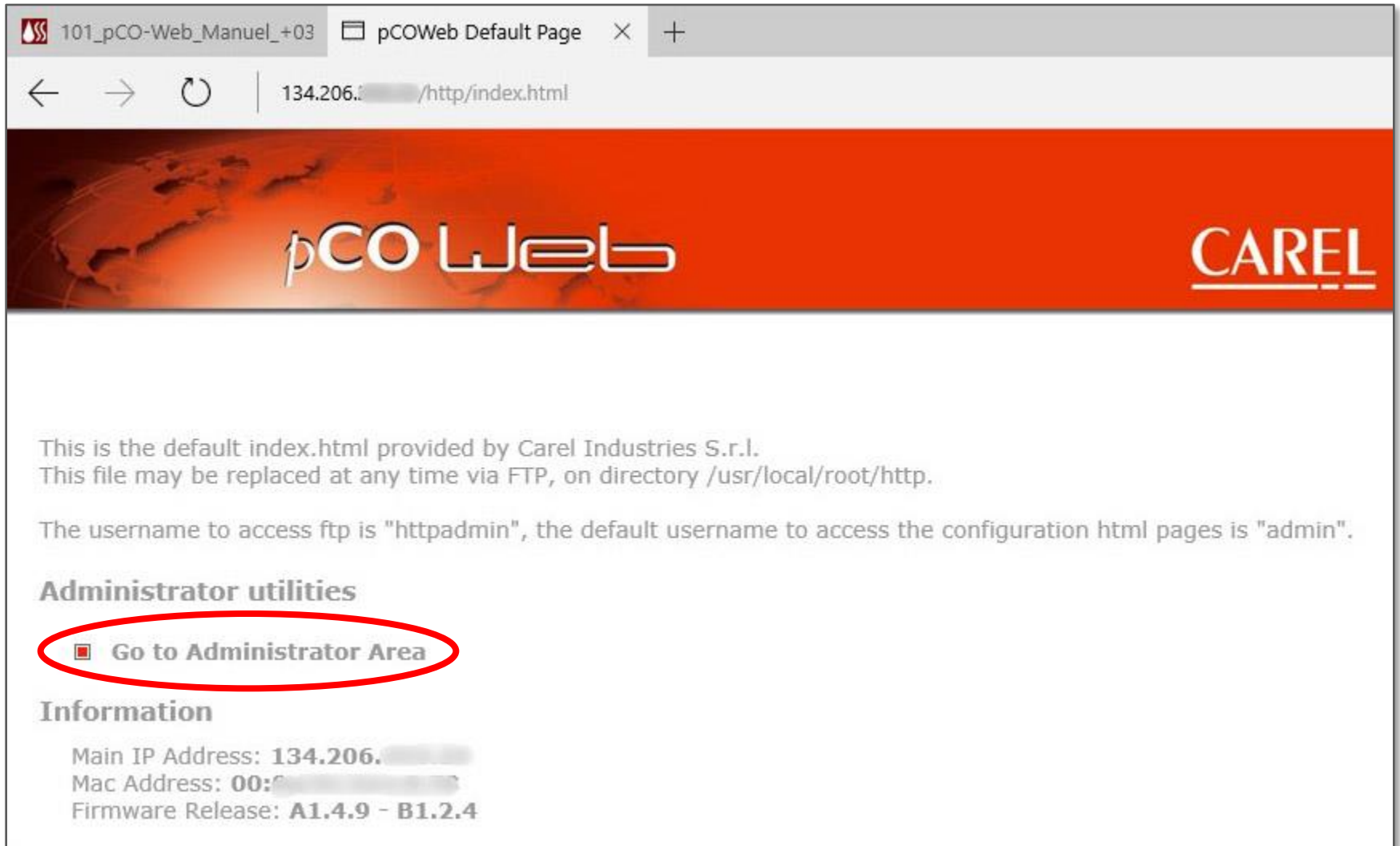
➤ Mode admin, the default settings are:

Username : admin

Password : fadmin

« Sécurité » des objets connectés

Exploration



101_pCO-Web_Manuel_+03 pCOWeb Default Page × +

← → ↻ | 134.206.100.100/http/index.html

pCO Web **CAREL**

This is the default index.html provided by Carel Industries S.r.l.
This file may be replaced at any time via FTP, on directory /usr/local/root/http.

The username to access ftp is "httpadmin", the default username to access the configuration html pages is "admin".

Administrator utilities

- [Go to Administrator Area](#)

Information

Main IP Address: 134.206.100.100
Mac Address: 00:0C:29:00:00:00
Firmware Release: A1.4.9 - B1.2.4

« Sécurité » des objets connectés

Exploration

The screenshot shows a web browser window with the address bar displaying "134.206.../config/adminpage.html". The page header features the "pCO Web" logo and the "CAREL" logo. A navigation menu includes "Information", "Configuration", "Clock and Logger", "Events", "Tests", "Customer Site", and "Info & Contact". The "Configuration" section is active, with sub-tabs for "General", "Network", "pCO Com", "SNMP", "BACnet", "Plugins", "Users", and "Firmware". The "Serial communication" page contains the following text:

pCOWeb is an optional card which can be fitted into a pCO controller and therefore, in order to communicate correctly with it, pCOWeb needs to be set up according to its settings. Changing these settings will not affect the IP functionalities of the card (SNMP, BACnet..) but only the communication between pCOWeb and pCO controller. Refer to the manual of the pCO application for further information on how to set up the communication protocols in the pCO. **Modify very carefully.**

Protocol: Carel

Baud Rate: 19200 (default 19200)

Submit

System is using:
User parameters

Firmware Release:
A1.4.9 - B1.2.4

Mac Address:
00:...

Copyright © 2003-2012 by Carel Industries S.r.l., Brugine (PD) - Italy. All rights reserved. Contact: pcoweb@carel.com

« Sécurité » des objets connectés

Exploration

The screenshot shows the pCO Web configuration interface. The browser address bar indicates the URL is 134.206.100.100/config/adminpage.html. The page title is "Summary Page" and it includes a note: "!! Data is live, it automatically updates every 5s !!". Below this, there is a navigation instruction: ">> Double click on a value to change it <<".

The interface features a sidebar on the left with navigation options: Information, Configuration, Clock and Logger, Events, Tests, Customer Site, and Info & Contact. The Info & Contact section includes a "Reboot" button and system information: "System is using: User parameters", "Firmware Release: A1.4.9 - B1.2.4", "Mac Address: 00:...", and "pCOWeb's date: 2016-03-24 09:57". There are also logos for W3C HTML 4.01 and BTL (Bachelier Test Laboratory).

The main content area displays three tables of variables:

- Digital Variables:** A table with 20 columns (Var Idx 1-20) and 10 rows. The value for Var Idx 1-207 is highlighted in blue.
- Analog Variables:** A table with 20 columns (Var Idx 1-20) and 10 rows. Values for Var Idx 1-207, 6.4, 2.4, and 4.2 are highlighted in yellow.
- Integer Variables:** A table with 20 columns (Var Idx 1-20) and 10 rows. The value for Var Idx 1-207 is highlighted in yellow.

At the bottom of the page, the copyright notice reads: "Copyright © 2003-2012 by Carel Industries S.r.l., Brugine (PD) - Italy. All rights reserved. Contact: pcoweb@carel.com". The system tray at the bottom right shows the time as 09:59 on 24/03/2016.

« Sécurité » des objets connectés

Exploration

Analog Variables

1-207

0.0	7.8	0.0	6.4	0.0	2.4	0.0
1.0	23.5	14.0	7.0	15.0	7.0	8.0
0.0	0.0	0.0	23.2	0.0	0.0	0.0
0.0	0.0	0.0	20.0	0.0	160.0	15.0
15.0	8.4	1.0	6.6	5.5	0.0	0.0
0.0	0.0	0.0	0.0	0.0	0.0	0.0
0.0	U	U	U	U	U	U
U	U	U	U	U	U	U
U	U	U	U	U	U	U
U	U	U	U	U	U	U

« Sécurité » des objets connectés

Piratage

The screenshot shows a web browser window titled "Carel pCOWeb - Microsoft Edge" with the address bar displaying "134.206. [redacted] /config/pw_demo.cgi?var_index=1&var_type=Analog". The page features a red header with the "pCO Web" logo. Below the header, there are two main sections: "Read variable from pCOx" and "Write variable to pCOx".

In the "Read variable from pCOx" section, there are two dropdown menus: the first is set to "70" and the second to "Analog". A "Read" button is located to the right of these menus. Below them, the text "Current value: 20" is displayed.

In the "Write variable to pCOx" section, there is a label "Variable Analog 70 new value:" followed by an input field containing the number "35". A "Write" button is located to the right of this input field and is circled in red. Below this, the text "Operation result: Undefined" is shown.

At the bottom of the page, there is an "Operation result legend:" section with the following items:

- Undefined : Last action issued did not need any pCOx answer
- Ok : pCOx sent back a value
- Timeout : pCOx did not send back any value

At the very bottom of the page, there is a "Close Window" link.

« Sécurité » des objets connectés

Nous ne sommes pas seul

The screenshot shows a Shodan search interface. The search query is "pcoweb port:23 country:FR org:". The results show a single device located in France, with IP address 91.250.250.1250. The device is running Linux 2.4.21-rmk1 (pCOWeb) (ttya3) and was added on 2018-03-17 18:18:13 GMT. The interface includes navigation tabs for Shodan, Developers, Book, and View All...; a search bar with the query; and buttons for Explore, Downloads, Reports, Exploits, Maps, Share Search, Download Results, and Create Report. The results are categorized by TOP COUNTRIES, TOP CITIES, and TOP ORGANIZATIONS.

Shodan Developers Book View All...

SHODAN pcoweb port:"23" country:"FR" org:" [REDACTED] [REDACTED]

Explore Downloads Reports

Exploits Maps Share Search Download Results Create Report

TOP COUNTRIES

France 1

TOP CITIES

[REDACTED] 1

TOP ORGANIZATIONS

[REDACTED] SA 1

Total results: 1

91. [REDACTED].250

250 [REDACTED].01 [REDACTED] SA

Linux 2.4.21-rmk1 (pCOWeb) (ttya3)

Added on 2018-03-17 18:18:13 GMT

France, [REDACTED]

Details

pCOWeb login:

« Sécurité » des objets connectés

Nous ne sommes pas seul



« Sécurité » des objets connectés

Conclusion

Protéger un objet connecté autant qu'un serveur :

- ▀ faire une recette de l'installation,
- ▀ réduire la visibilité (network IP séparé, filtres réseau, ...),
- ▀ limiter les accès (adresses IP des clients),
- ▀ invalider tous les protocoles et fonctions inutiles,
- ▀ gérer les comptes de connexions (invalider les comptes inutiles, changer les mots de passe),
- ▀ Mettre à jour les composants logiciels (firmwares, sites WEB, ...),
- ▀ ...