New SCADA Default Passwords added to DPE xml Database

Author : mastermind

Well, i spent this snowy sunday digging into few ICS (Industrial Control Systems) vendors documentation. And here is what i come up with.

- 4 Siemens WinCC 7.x passwords never heard about (or at least i got no information on google). Those are related to some Demo Accounts. I found them in a documentation called "Hardening Siemens WinCC 7.x". Siemens recommended to remove them from the Database.
    - winccd / winccpass
    - wincce / winccpass
    - DMUser / Data&Pass
    - Administrator / Administrator
- Siemens Synco Ozw Web Server was reported in a CVE-2012-3020 to handle unspecified default accounts. Well, digging in more Siemens documentation (SyncoTM, SyncoTM living Web server OZW772 V2.0 Commissioning instructions) leads to unreveal the default password.
    - Administrator / Password
- I choose randomly 2 ICS vendors just to prove that SCADA systems security is a nonsense
    - Moxa www.**moxa**.com
        - 2 default passwords in a bunch of Series Railway Remote I/O (ioLogik E12xx , ioLogik E15xx) just to name a few.
            - Http on Port 9020 . username = none / password = root
            - Http on Port 9020 . username = none / password = none
        - 2 default passwords in a bunch of Cellular Micro RTU Controller (ioLogik W53xx, ioLogik)

- through ioAdmin Tool. username=administrator / password=.... let me see .. blank ..yup you got it. By the way ioAdmin Tool could be downloaded at http://www.moxa.com/support/DownloadFile.aspx?type=support&id=1149
- Telnet on port 9900 / 9000. username = root / password root

- Now, this is my favorite. IA240/241 Embedded computer. It's a linux based system. And guess what, it ships with a vulnerable FTP server (ftp server wu-2.6.1) according to documentation screenshots. Anyway, you dont need to fire up metasploit and craft your payload. Here a the default password (50 ways to leave your lover). Sorry, for those who are seeking for the challenge :)
  - telnet root / root
  - ftp root / blank
  - ppp root / blank
  - serial console root / root
- Some story for this one ioPAC 8020-C

- westermo www.**westermo**.com
  - Tele modem TDW-33 has 2 default accounts.
    - normal dial-up password is "blank"
    - remote configuration (with a call back) password "n3Y9kA6otYZu8". This one is hard coded and could be used by Westermo Support (nothing confirmed but i need to dive more into this one. **It could be very serious**

I still have a tons of documentation to read. Will keep you update.

One more thing, i updated the DPE - Default Password Enumeration (both Parser (now returns the CVE) and DB) to reflect the changes with these new additions (i also added Sinapis astridservice & 36e44c9b64 passwords)