Tetra Industriële Security

Gebruikersgroepvergadering

07 / 05 / 2015

Eerste overzicht zwaktes

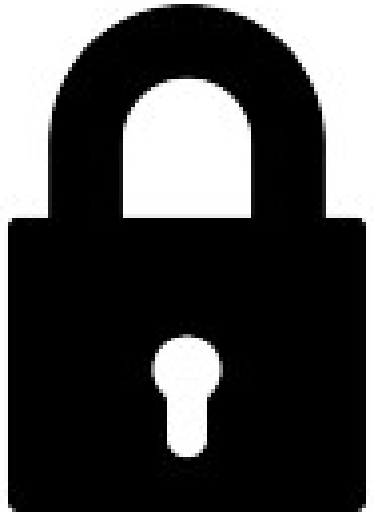
Systemen

- Een industrieel netwerk is een mengelkroes van toestellen:
  - Industriële Switches, volledig beheerbaar en met gemakkelijke website
  - Human Machine Interfaces met daarachter een (Windows) PLC die een GUI aanbiedt
  - Reguliere PLC’s die motoren en dergelijke aanstuurt met een eigen protocol
- Wij wensen ons niet te beperken tot één type of vendor en bekijken alles **objectief**

De eerste demo’s

We hebben drie types toestellen van drie vendors geselecteerd en reeds enkele ‘problemen’ gevonden:

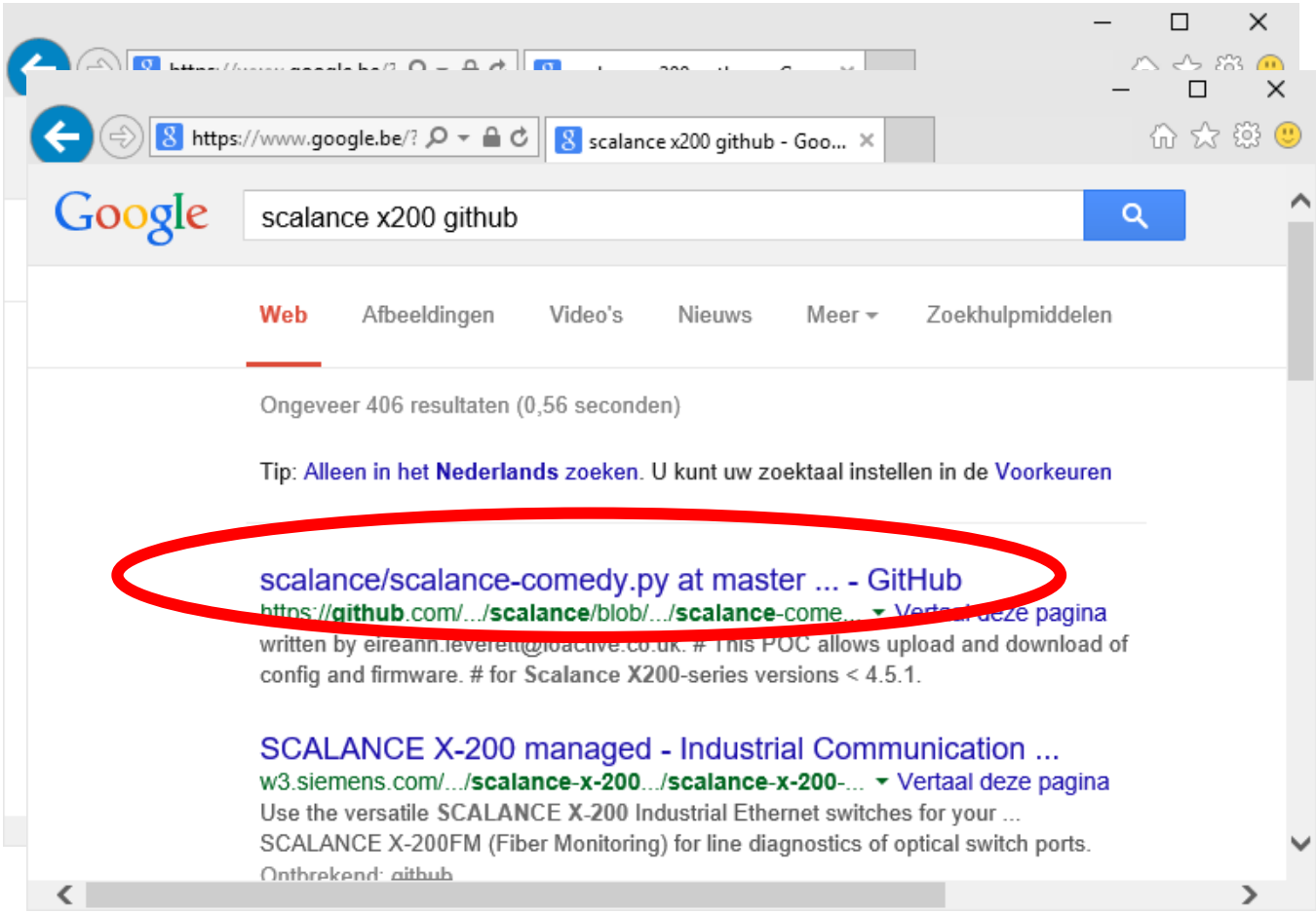
- Siemens Scalance X-200 Industrial Switch
- Beckhoff CX9020 WinCE 7 PLC met DVI-poort
- Phoenix Contact PLC ILC 150 ETH



Siemens Scalance X-208

Siemens Scalance X-200 Switch

- Hoe te beginnen?
  - Eerste werk: Google!
- Gevonden probleem
  - *Unauthenticated Access*
  - CVE-2013-5944b
  - Begin 2013 gemeld
  - Ook voor X-200IRT
  - Auteur: *Eireann Leverett*



Demo Scalance X-208

Oplossing

- Probleem eerst gemeld aan Siemens, die een update uitbracht op 18 Augustus 2013 (X-200 Firmware v4.5.1)
  - Gedemonstreerd op een conferentie in December 2014 en op YouTube
  - Iedereen dient zelf, manueel, de firmware up te daten.
    Dit betekent echter een reboot van het toestel …
- Probleem opgelost?
  - Toch voor even …
  - Totdat we dit opmerkten
    http://www.siemens.com/innovation/pool/de/forschungsfelder/siemens_security_advisory_ssa-954136.pdf

SSA-954136: User Impersonation Vulnerability in SCALANCE X-200IRT Switch Family

Publication Date	2015-02-02
Last Update	2015-02-02
Current Version	V1.0
CVSS Overall Score	5.3

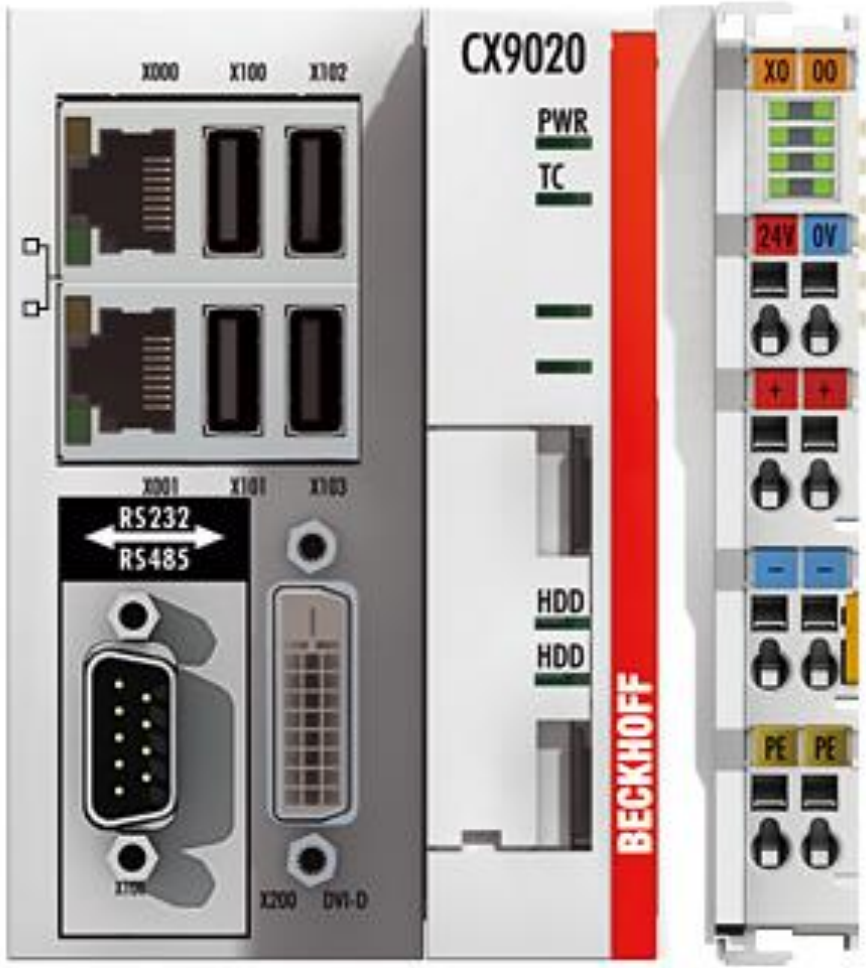
Summary:

The latest firmware update for the SCALANCE X-200IRT switch family fixes a vulnerability which could allow attackers to impersonate legitimate users of the web interface.

AFFECTED PRODUCTS

- SCALANCE X-200IRT switch family: All versions < V5.2.0

Beckhoff CX9020



Inside Information

- Via-via (collega pentesters) kregen we niet-functionele code om ons op weg te helpen
  - Eerder onderzoek opnieuw uitgevoerd én uitgebreid
  - Gemigreerd naar een uitgebreid, zelf geschreven Python script
- Gevonden problemen
  1. Website zonder Cookies of Session ID's
     - Zogenaamde *zero-day*: er is tot op heden **geen** oplossing van de vendor (later meer)
  2. Remote Access zonder credentials 'by design' (later meer)

Beckhoff Web Vulnerability

- Voor zover gekend nog geen CVE-code:
  - CX9020 (en ook andere CX-PLC's) hebben een website: http://<IP-adres>/config (met default credentials *guest* / *1*)
- Elke PLC heeft een unieke zogenaamde UNS code, die uitgewisseld wordt bij authenticatie, deze kan echter worden uitgelezen via een SSDP-bericht **zónder authenticatie**
- Ons script leest dit in en kan automatisch de PLC herstarten of gebruikers toevoegen of …

Demo Beckhoff CX9020

Oplossing?

- Probleem is gekend bij Beckhoff
- Binnenkort (wellicht) update van de firmware.
- Intussen: webserver volledig uitzetten en/of
  toestel afschermen van het netwerk
- Maar er is meer, we vonden ook dit
  http://download.beckhoff.com/download/Document/IndustPC/Advisory-2014-001.pdf

Advisory 2014-001: Potential misuse of several administrative services

Solution

This can either be solved by:

- Updating to images build >= 10/22/2014 solves this by disabling the services by default
- The configuration of the web server pathes can be found in the Windows registry at the path “HKEY_LOCAL_MACHINE\COMM\HTTPD\VROOTS\”. To disable the Windows CE Remote Configuration Tool delete the subtree “/remoteadmin”.
- Disable startup of CE Remote Display service (cerdisp.exe) with deleting the registry key containing the “CeRDisp.exe“ [-HKEY_LOCAL_MACHINE\init\Launch90]
- Disable telnet by setting the registry key [HKEY_LOCAL_MACHINE\Services\TELNETD\Flags] to dword:4
- The IPC Security Manual [1] provides information for securing the environment of an EPC.

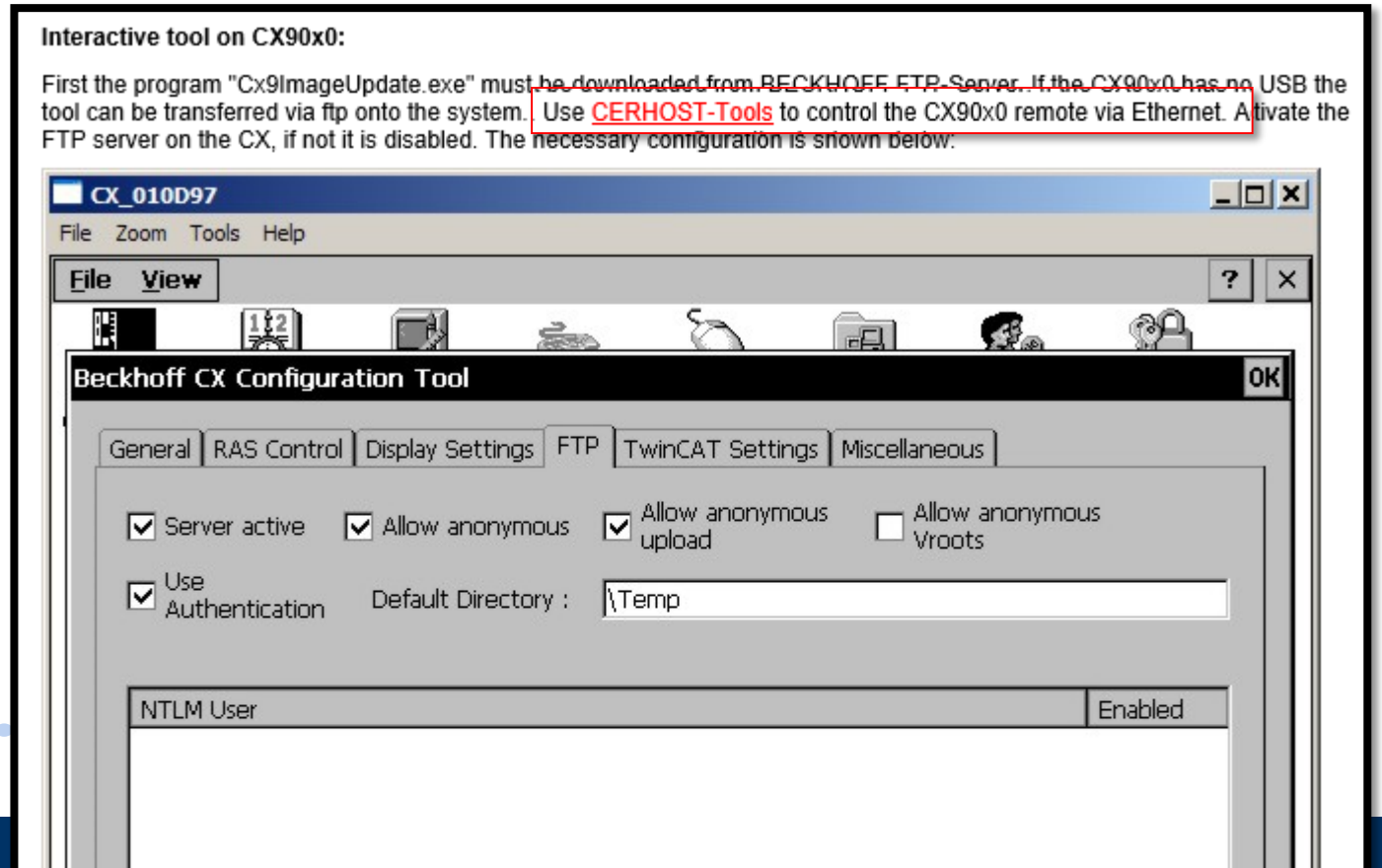
Reporting vulnerabilities

Beckhoff Automation welcomes responsibly coordinated reports of vulnerabilities and Beckhoff will collaborate with reporting parties to fix vulnerabilities or mitigate threats.

corresponding network ports (TCP 80/987/23). This implies that the services are running.

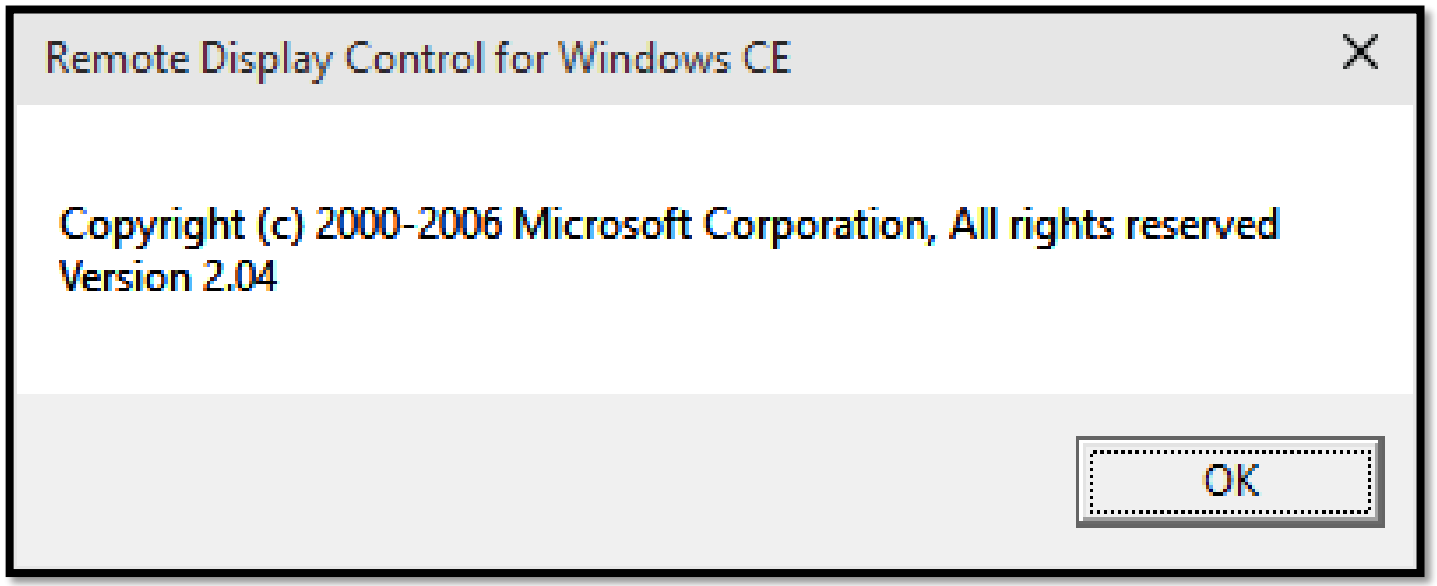
Beckhoff tweede probleem, poort 987

- Een blik op de online handleiding van Beckhoff



CERHOST

- Een tool van **Microsoft** om Windows CE op afstand te beheren.
- Niet langer in ontwikkeling
- Microsoft zegt: DO NOT USE



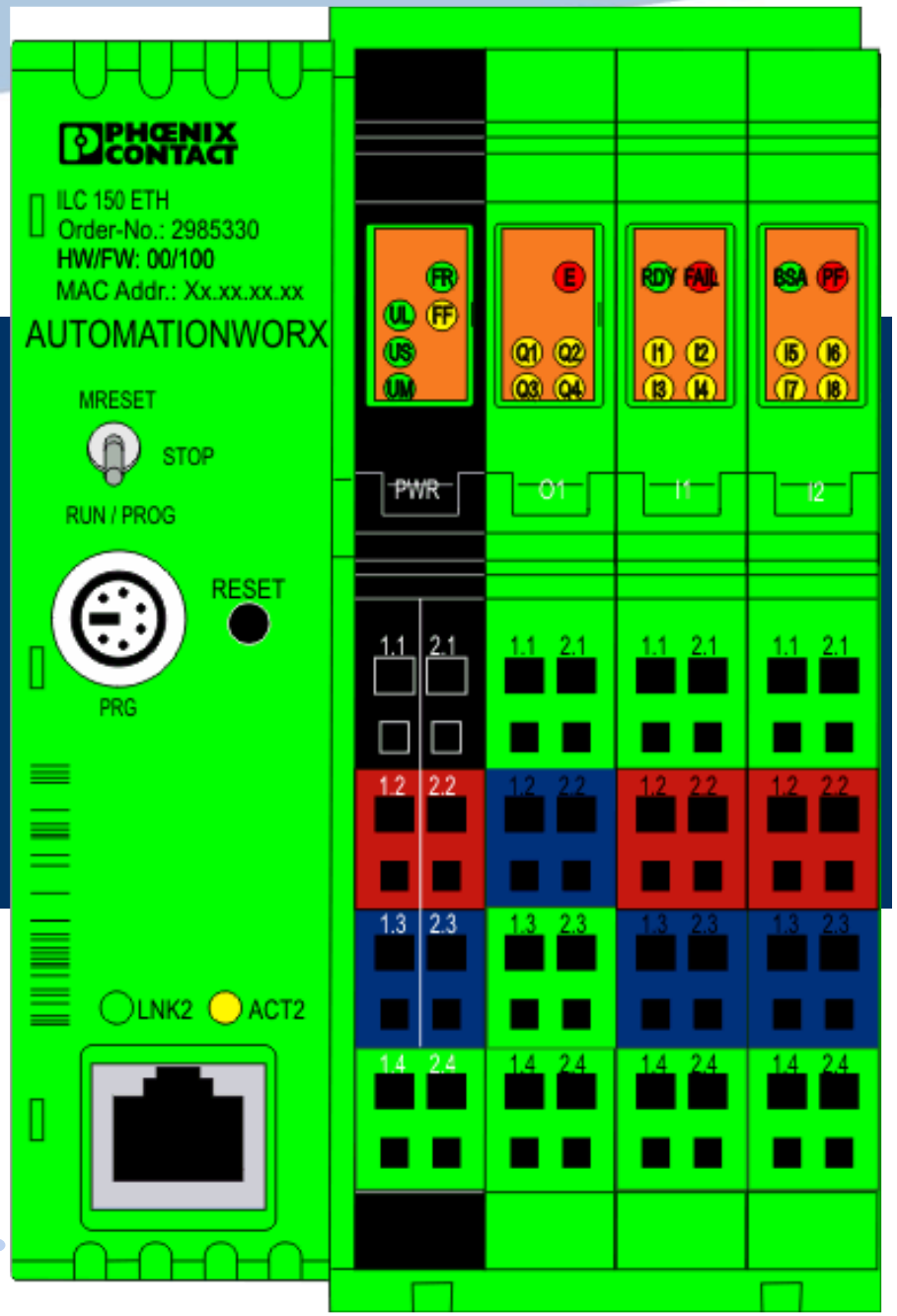
- Getest met **recentste** firmware op o.a. CX9010

DEMO Win CE met CER Display

Oplossing?

- Probleem is gekend bij Beckhoff
- Beste oplossing: **netwerk afschermen**!
- Zie eerdere presentaties ☺

Phoenix Contact ILC 150 ETH



Hoe te werk

- Opnieuw op zoek naar eventuele problemen
- Weinig ‘bugs’ in de software,
  omwille van een beperkte Ethernet functionaliteit
  - Wel (read-only) FTP toegang met project gegevens
- Toch vrij snel dit gevonden
  https://www.phoenixcontact-software.com/en/company/news/news-press/details/items/243
- Gekend als CVE-2014-9195

PHOENIX CONTACT SOFTWARE OFFERS MITIGATION ADVICE FOR PROCONOS AND MULTIPROG AUTHENTICATION VULNERABILITY ICSA-15-013-03/ICS-

VULNERABILITY OVERVIEW

MISSING AUTHENTICATION[a]

The protocol behind the application software does not have an authentication mechanism. This allows anyone with network access to inject commands to the protocol.

CVE-2014-9195[b] has been assigned to this vulnerability. A CVSS v2 base score of 10.0 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:C/I:C/A:C)[c].

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability could be exploited remotely.

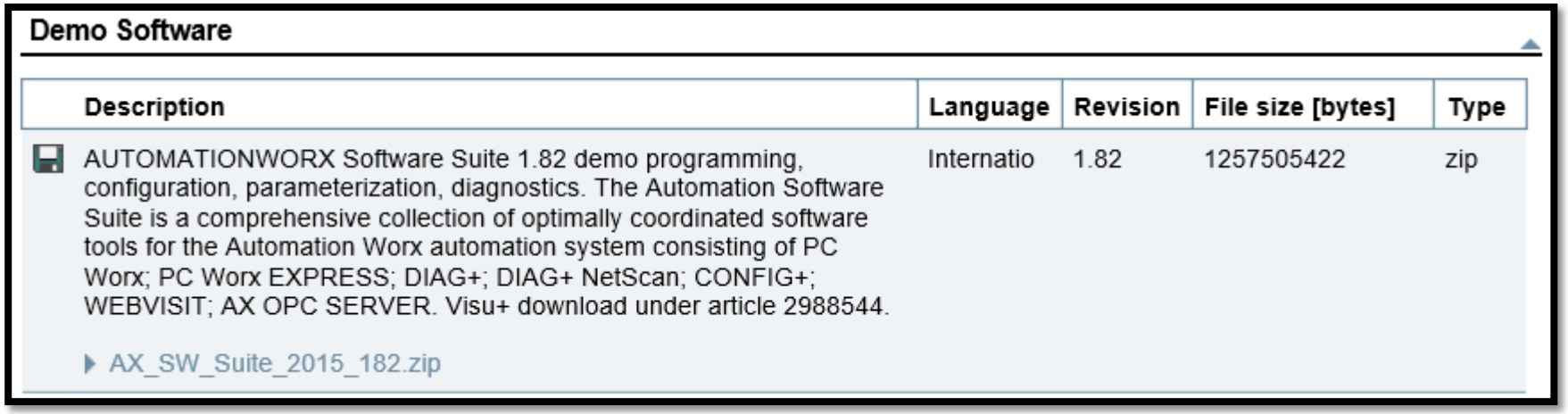
EXISTENCE OF EXPLOIT

No known public exploits specifically target this vulnerability.

The identified vulnerability allows for unauthenticated users to modify programs in some controllers that are utilizing ProConOs and MULTIPROG products. Unauthenticated users must have network or physical controller access to exploit this vulnerability. This version affects all versions of ProConOS and MULTIPROG from Phoenix Contact Software (formerly KW-Software).

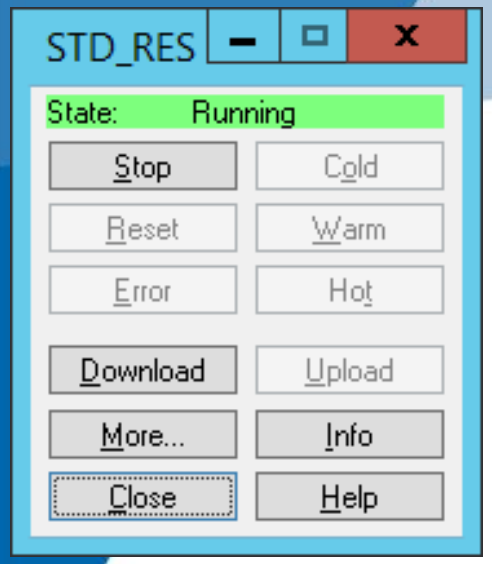
Phoenix Contact PLC Software PC Worx

- In de praktijk vrij ‘simpel’ probleem:
  - Iedereen met een Windows PC kan de software *PC Worx* installeren
    - Echter: de gratis Express versie kan geen PLC’s aansturen, wel simuleren
    - De volledige software kan als demo worden gedownload (1,2GB)



Demo Software

Description	Language	Revision	File size [bytes]	Type
AUTOMATIONWORX Software Suite 1.82 demo programming, configuration, parameterization, diagnostics. The Automation Software Suite is a comprehensive collection of optimally coordinated software tools for the Automation Worx automation system consisting of PC Worx; PC Worx EXPRESS; DIAG+; DIAG+ NetScan; CONFIG+; WEBVISIT; AX OPC SERVER. Visu+ download under article 2988544. ▸ AX_SW_Suite_2015_182.zip	Internatio	1.82	1257505422	zip



PC Worx

- In PC Worx zelf is het een kwestie van een leeg project te maken, het IP van de PLC in te geven en het controlepaneel te starten.
  - Daarna kan de PLC aangestuurd worden met Stop en diverse Start methodes en eventueel zelfs een nieuw (gecompileerd) project uploaden

- Plan van aanpak?
  - Onderscheppen van alle verkeer en protocol (proberen te) begrijpen
  - Vervolgens zelf programmeren (opnieuw Python)

Phoenix Contact PLC resultaten

- Simpel script om PLC details uit te lezen
  - Gebeurd op poort 1962
  - Toont PLC Type, Firmware versie en Firmware Build Timestamp
- Simpel script om PLC status uit te lezen
  - Gebeurd op poort 41100
- Simpel script om PLC te controleren (Stop, Cold/Warm/Hot Start)
  - Gebeurd op poort 41100

DEMO Phoenix Contact ILC 150 ETH scripts

Verder?

- Wellicht is het mogelijk om ook effectief gecompileerde projecten (bin-files) te ‘downloaden’, sturen naar PLC
  - Nog geen demo-script hiervoor ☹

Oplossing?

- Probleem is gekend bij Phoenix Contact
- Beste oplossing: **netwerk afschermen**!
- Zie eerdere presentaties ☺
- Of zoals Phoenix Contact het zelf zegt:

https://www.phoenixc... Phoenix Contact Software o...

Mitigation:
Phoenix Contact Software recommends that users implement an adequate defense–in-depth networking architecture for control systems where these devices are operating. The use of virtual private networks (VPNs) is highly recommended for remote access, as well as the use of firewalls for network segmentation or controller isolation when required.
Automation suppliers might use the ProConOS open protocol layer to update their automation devices with a new firmware version implementing own authentication mechanism.

Acknowledgement:
Phoenix Contact would like to thank Reid Wightman of Digital Bond and ICS-CERT for a coordinated release of this vulnerability.

Resources:
Recommended security practices by ICS-CERT:
http://ics-cert.us-cert.gov/content/recommended-practices

Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies
https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/Defense_in_Depth_Oct09.pdf

For more information about the official ICS-CERT advisory please refer to:
https://ics-cert.us-cert.gov/advisories/ICSA-15-013-03

Dank u voor uw aandacht

Vragen ?