Vulnerabilities

Architecture

Attack Surface

Real Examples

Suggestions

Attacks
Effects
Solutions

**ICS Threat Scenarios**

Luigi Auriemma

September 2015

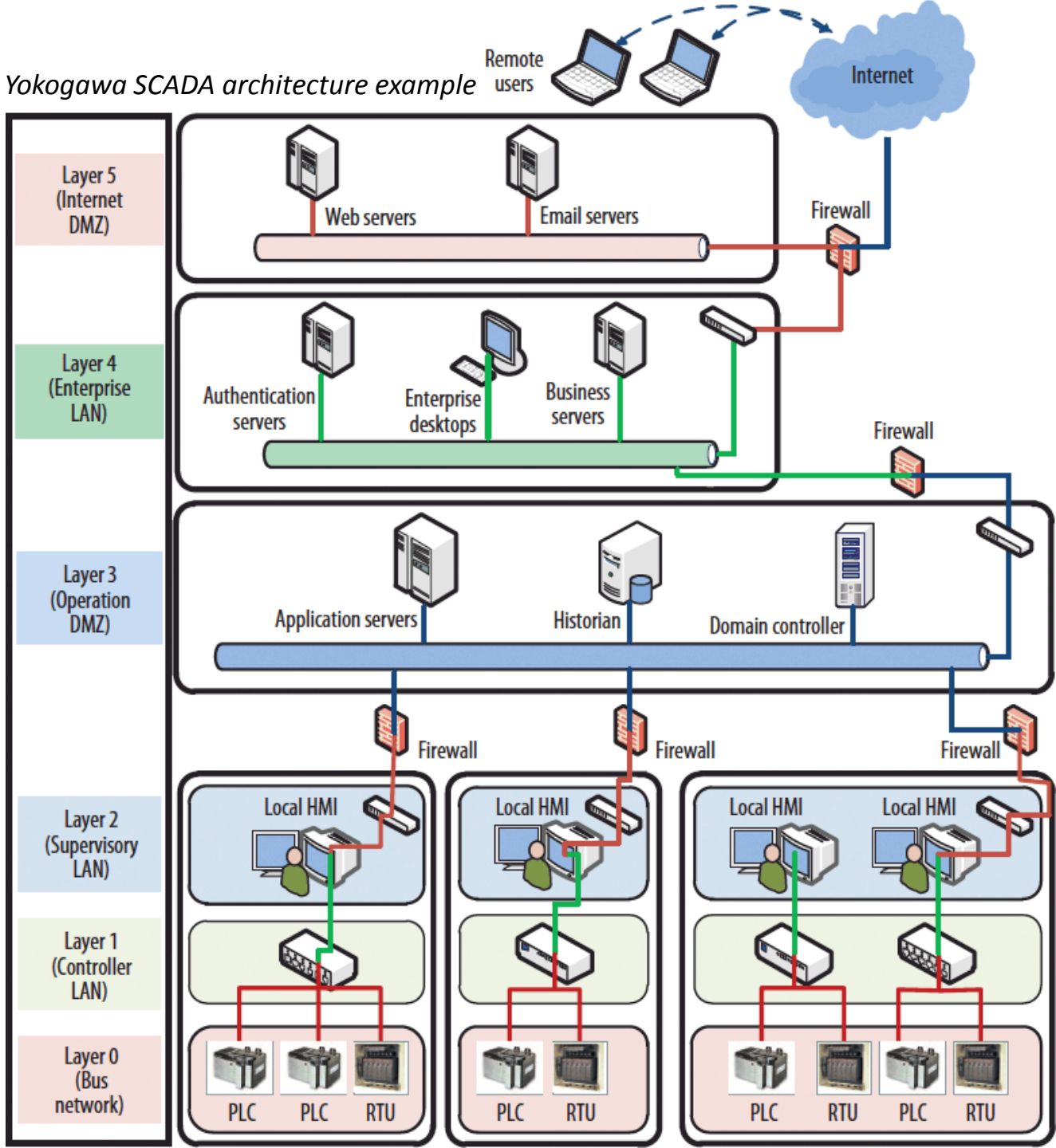
# SCADA architecture

Every situation is different because it's an highly customized environment in which are used different types of:

- Connections
- Protocols
- Devices
- Software
- Security procedures
- Security products *(firewall, AV, IDS)*
- Solutions

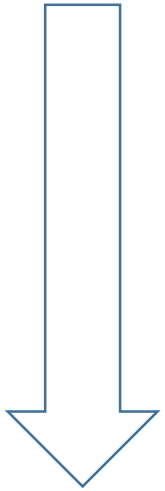
What's sure is that more devices will be connected via TCP/IP, and so, it's more easy to get reached by possible attackers.

*Yokogawa SCADA architecture example*

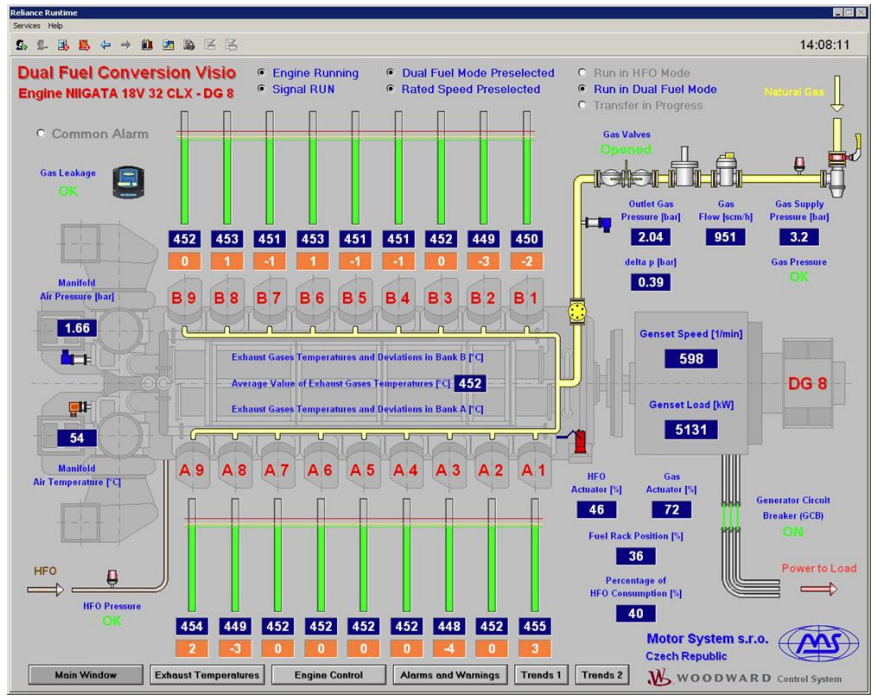


# TARGETS

**Operating System**
**&**
**General Software**



- Security vulnerabilities
- Design issues
- Bad security practices
- Old software versions




**PLC / RTU / DCS devices**
**&**
**HMI / SCADA**

- Siemens
- General Electric
- ABB
- Rockwell
- Invensys / Wonderware
- Schneider Electric
- Indusoft
- Codesys
- Iconics

Kernel vulnerabilities


Old versions necessary for some SCADA products

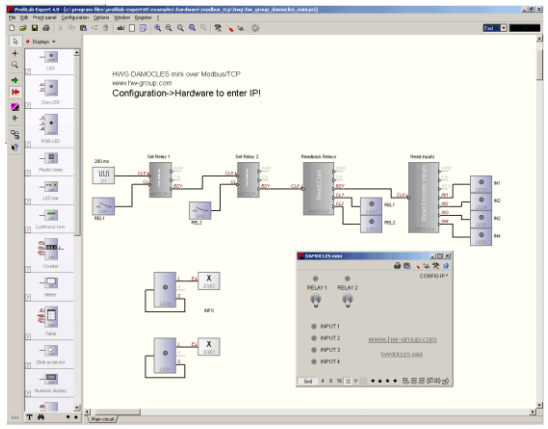




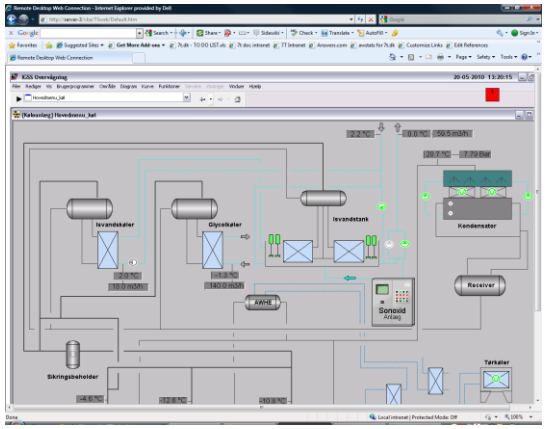
# HMI/SCADA ATTACK SURFACE

Server-side vulnerabilities through TCP and UDP open ports

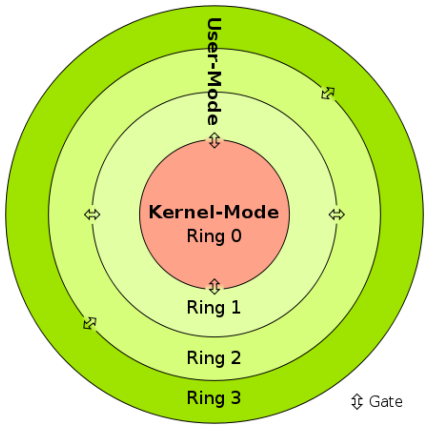
Handling of project files and other files with registered extensions



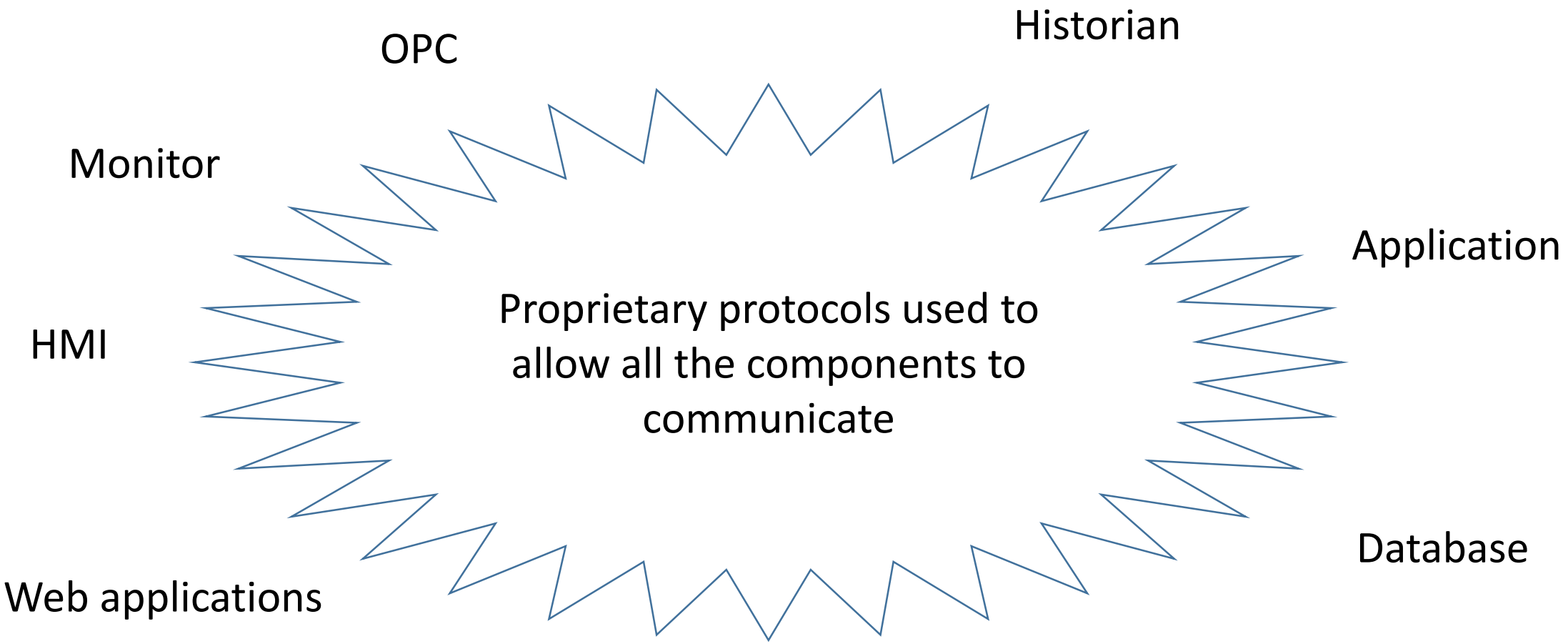

Client-side vulnerabilities through the integration in web browsers: *ActiveX* and *URL protocols*



Local privilege escalation with processes and services running as SYSTEM or Administrator



# Server-side protocols




The code is usually poorly written and tested… or ...

# Server-side protocols

## Advisory (ICSA-11-264-01)

### AzeoTech DAQFactory Stack Overflow

Original release date: September 21, 2011 | Last revised: January 24, 2014

This advisory is a follow-up to the alert titled "ICS-ALERT-11-256-02—AzeoTech DAQFactory Stack Overflow" that was published September 13, 2011, on the ICS-CERT web page.

ICS-CERT is aware of a public report of one stack overflow vulnerability with proof-of-concept (POC) exploit code affecting AzeoTech DAQFactory, a SCADA/HMI Product. According to the report, the vulnerability is exploitable via a service running on Port 20034/UDP. The report was released without coordinating with either the vendor or ICS-CERT. ICS-CERT has coordinated with AzeoTech, which has produced an upgrade that resolves the vulnerability. ICS-CERT has not validated the upgrade.

Attribution for the vulnerability discovery is not provided in this advisory because no prior coordination occurred with the vendor, ICS-CERT, or other coordinating body. ICS-CERT encourages researchers to coordinate vulnerability details before public release. The public release of vulnerability details prior to the development of proper mitigations may put industrial control systems (ICSs) and the public at avoidable risk.

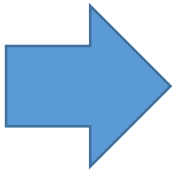
### Mitigation

According to AzeoTech, the vulnerable feature has been completely removed in the next version (Version 5.86). The feature was undocumented, and AzeoTech does not believe it was being used by any of their customers. Therefore, its removal should not adversely affect any DAQFactory users.

… or not meant for the final product!

# Hardcoded accounts, passwords and keys

PLC firmware
or
SCADA software



```
package com.schneiderautomation.misc;

import java.applet.Applet;

public final class GlobalConfig
{
  public static int MIN_POLLING_DELAY = 10;
  public static int MAX_POLLING_DELAY = 10000;
  private static String m_ftpRoot = "";
  private static String m_ftpLogin = "sysdiag";
  private static String m_ftpPassword = "factorycast@schneider";
  private static String m_passFile = "/rdt/password.rde";
```

Left in the code due to design errors, maintainance accounts, backdoors or just forgotten there by mistake!

**Advisory (ICSA-12-263-02)**

ORing Industrial Networking IDS-5042/5042+ Hard-Coded Credential Vulnerability

Original release date: September 19, 2012 | Last revised: April 22, 2013

**Advisory (ICSA-12-018-01B)**

Schneider Electric Quantum Ethernet Module Hard-Coded Credentials B)

Original release date: September 23, 2013 | Last revised: February 14, 2014

**Advisory (ICSA-15-160-01)**

N-Tron 702W Hard-Coded SSH and HTTPS Encryption Keys

Original release date: June 09, 2015 | Last revised: July 01, 2015

**Advisory (ICSA-15-181-02 )**

SMA Solar Technology AG Sunny WebBox Hard-coded Account Vulnerability

Original release date: September 03, 2015

**Advisory (ICSA-12-354-01A )**

Ruggedcom ROS Hard-Coded RSA SSL Private Key

Original release date: April 29, 2013 | Last revised: March 06, 2014

**Alert (ICS-ALERT-15-224-01)**

KAKO HMI Hard-coded Password

Original release date: August 12, 2015

**Advisory (ICSA-13-136-01)**

TURCK BL20 and BL67 Programmable Gateway Hard-Coded User Accounts

Original release date: May 16, 2013 | Last revised: December 23, 2013

**Advisory (ICSA-12-354-01A )**

Ruggedcom ROS Hard-Coded RSA SSL Private Key (Update A)

Original release date: April 29, 2013 | Last revised: March 06, 2014

**Advisory (ICSA-14-205-01)**

Morpho Itemiser 3 Hard-Coded Credential

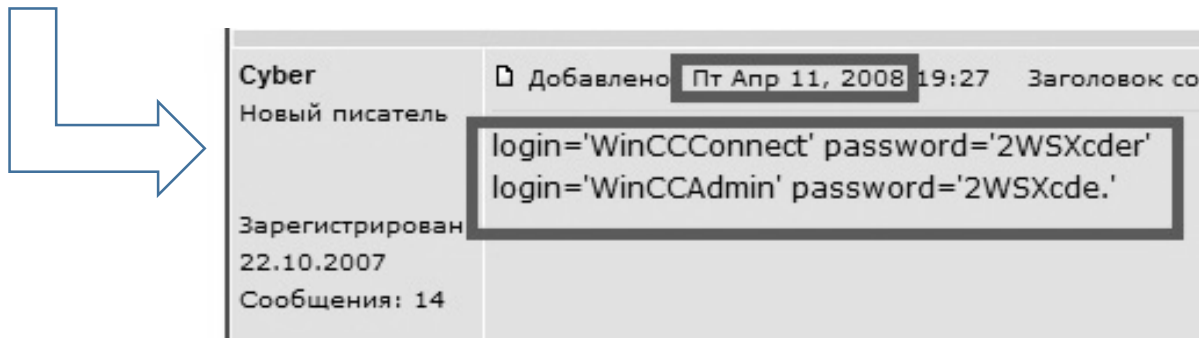
Original release date: July 24, 2014

**Advisory (ICSA-12-297-02)**

Korenix Jetport 5600 Series Hard-coded Credentials

Original release date: October 23, 2012 | Last revised: December 31, 2013

It’s a very diffused problem…
Even exploited by Stuxnet



# History of the Siemens WinCC default SQL Server password abused by Stuxnet for infection

## 2006

Wincc Database problem

Created by: Duncan at: 7/24/2006 11:21 AM (22 Replies)

Rating ☆☆☆☆☆ (0)
Thanks 0

Actions | New post

23 Entries  Entries per page: 10 | 20 | all  |< < 1 | 2 | 3 > >|

7/24/2006 11:21 AM  Rate ☆☆☆☆☆ (0)

Duncan

Member

Joined: 6/14/2006
Last visit: 1/12/2007
Posts: 22
Rating:
★★★★★ (1)

Hi Friends,

I am facing a problem with wincc.Whenever I try to open an existing project it gives me error saying the related **.mcp file could not be loaded and error 0x80046127**.
Also in Simatic manager environment an error is coming which says **wincc objects cannot be edited(possible causes:1.The required database is not installed,2.The required access rights are not available)..**

I have checked the authentication in security od SQL server its is set at mixed(sql server and windows)..

Could you please provide mesome pointers to get out of this problem..

Note:I am working with wincc of PCS7 environment

Thanks in advance..
Duncan.

## 2008

Cyber
Новый писатель

Зарегистрирован 22.10.2007
Сообщения: 14

Добавлено Пт Апр 11, 2008 19:27  Заголовок сообщения:

login='WinCCConnect' password='2WSXcder'
login='WinCCAdmin' password='2WSXcde.'

|< < 1 | 2 | 3 > >|

4/15/2008 9:31 PM  Rate ☆☆☆☆☆ (0)

Dec

Gold Expert

Joined: 5/19/2006
Last visit:

Hey Cyber,
Are we suppose to congratulate you for cracking those passwords?
Those accounts/passwordsweremainlydesigned to ensure the use of a genuine MS-SQLsetup from WinCC Delivery CD/DVDand not a customer purchased version of MSSQL (see EULA).

Dec

## 2010

Stuxnet takes advantage of a hard-coded default password in Siemens Simatic WinCC software (CVE-2010-2772). The password allows privileged access to a back-end WinCC database. Once connected to the database, Stuxnet injects a copy of itself into the database, thereby infecting the PC running the WinCC database.

- CVE-2010-2772 Siemens SIMATIC WinCC Default Password Security Bypass Vulnerability

This enables the attacker to view the projects database and information from the WinCC server. It can alter configuration settings and can access or delete the file %ALL USERS PROFILE%\sqlx.dbi. Since .DBI files are database explorer information files, this deletion is most likely done to remove any trace of modification done by the malware in the database.

## 2012

**Advisory (ICSA-12-205-01)**

Siemens WinCC Insecure SQL Server Authentication

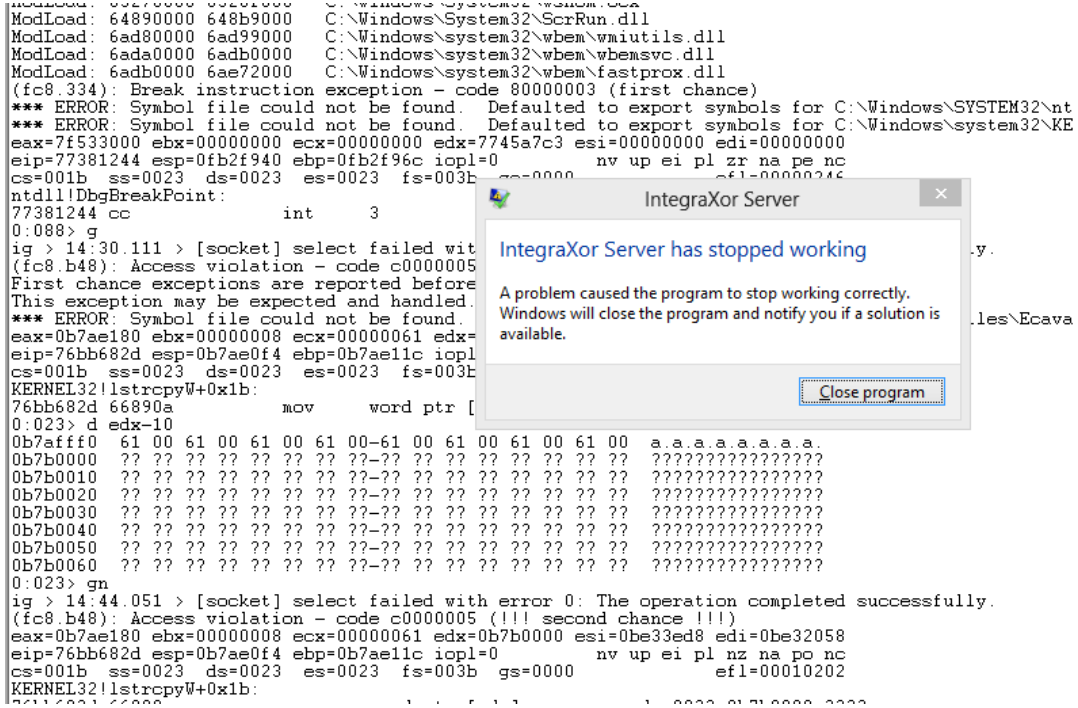
Original release date: July 23, 2012 | Last revised: May 08, 2013

### Overview

Siemens has released a software update for an insecure SQL server authentication vulnerability in Siemens' SIMATIC WinCC and SIMATIC PCS 7 software. Previous versions of SIMATIC WinCC use default SQL server credentials that allowed administrative access to the database. The default credentials cannot be changed or disabled. This vulnerability can be remotely exploited, as was the case with Stuxnet malware which was known to target this vulnerability. Siemens has produced an updated version that resolves the reported vulnerability.

# Memory corruption vulnerabilities

- Stack based buffer-overflow
- Heap overflow
- Integer overflow
- Format string
- Array overflow/underflow
- Write a byte/long at relative locations
- Write a byte/long at arbitrary locations
- Use-after-free (project files)
- Double free (project files)




Example:

CVE-2011-5007 – 3S CodeSys buffer-overflow

…

Why is it interesting?

# Effects

- Code Execution
- Denial of Service in case of failure

# Memory corruption vulnerabilities

| ABB | Vulnerability Security Advisory | | | |
|---|---|---|---|---|
| ABB Doc Id: 9ADB005083 | Last edit date | Lang. | Rev. | Page |
| ABB-VU-DMLD-AC500CPUFW-1386 | 2012-04-20 | English | A | 1/2 |

## ABB-VU-DMLD-AC500CPUFW-1386: Advisory for AC500 webserver

### Overview

ABB is aware of a buffer overflow vulnerability in the webserver component of the AC500 PLC. Affected customers were informed by their local sales units after a patch was made available in December of 2011. This advisory completes the publication process.

CVSS Overall Score: 6.4
CVSS Vector: AV:N;AC:L;Au:N;A:C;I:N;C:N;E:F;RL:OF;RC:C

### Affected Products

All AC500 CPU modules with firmware version **V2.1.3 and enabled** webserver:

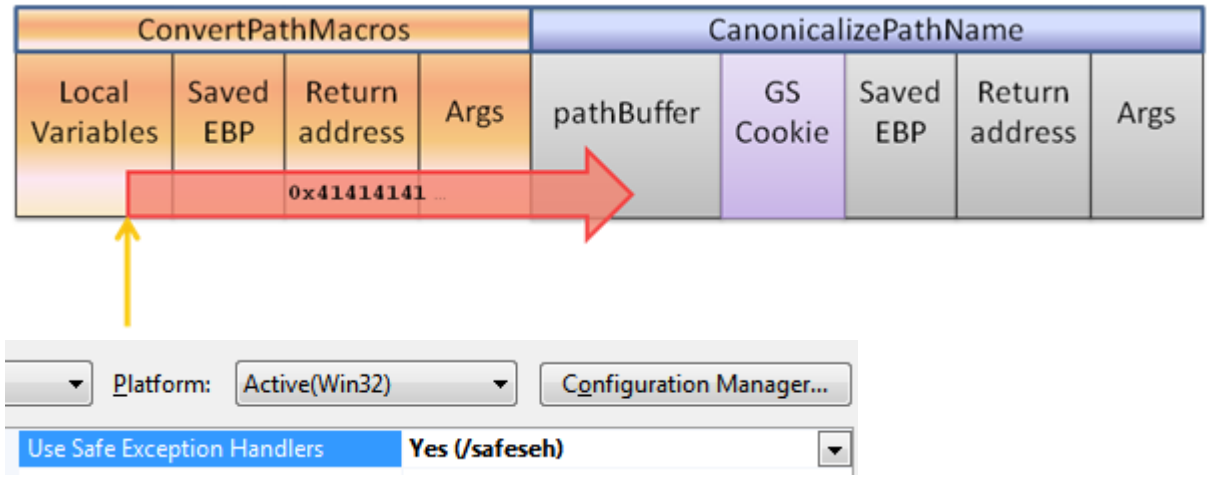
1SAP130 300 R0271 PM573-ETH
1SAP140 300 R0271 PM583-ETH
1SAP150 000 R0271 PM590-ETH
1SAP150 100 R0271 PM591-ETH
1SAP150 200 R0271 PM592-ETH
1TNE968 900 R0110 PM554-T-ETH
1TNE968 900 R1110 PM564-T-ETH
1TNE968 900 R1210 PM564-R-ETH
1TNE968 900 R1211 PM564-R-ETH-AC

### Acknowledgement

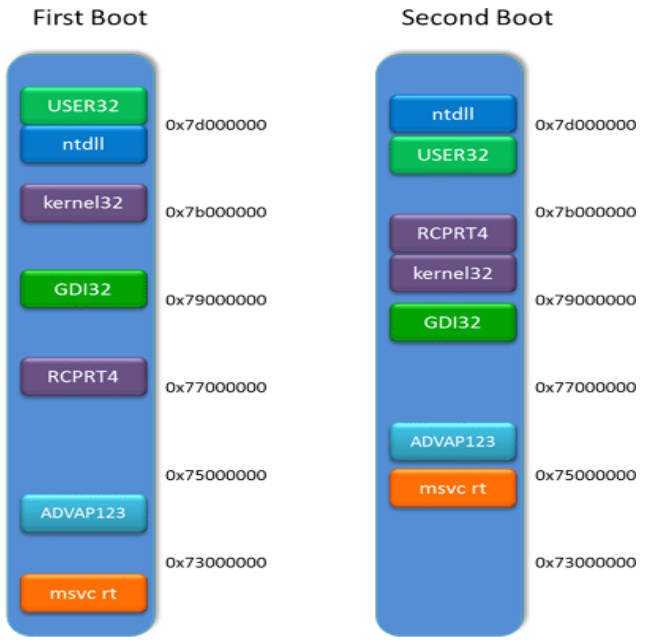
ABB would like to acknowledge Luigi Auriemma for finding the original bug in the CoDeSys webserver component (ICS-ALERT-11-336-01).
Further investigation and follow up by ABB revealed that contrary to the vulnerability of the PC version of the webserver, the PLC version does **not** allow injected code to be executed.

Example:
CVE-2011-5007 – 3S CodeSys buffer-overflow
…
Why is it interesting?
Because the issue was in a library used also on ABB PLCs!
*(ICSA-12-006-01 and ICSA-12-320-01)*

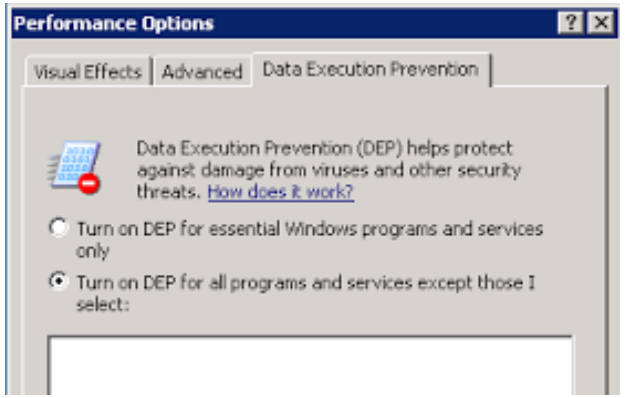
## Stack protections and secured exception handlers




## ASLR
## Address Space Layout Randomization




## DEP
## Data Execution Prevention




There are ways to limit the exploitation of these issues.

BUT the software is usually built without stack protections and with DEP and/or ASLR disabled in modules allowing the exploitation of the vulnerabilities.

Information disclosure vulnerabilities

- Directory traversal, like ..\..\..\DATA.INI
- Arbitrary files download, like C:\PATH\DATA.INI
- Memory disclosure

Examples:
CVE-2011-4878 – Siemens WinCC Flexible HmiLoad and miniweb directory traversal

CVE-2011-4051 – Indusoft WebStudio CEServer full remote file access

Effects

- Stealing information and sensitive data

# Information disclosure vulnerabilities

CVE-2011-4051 – Indusoft WebStudio CEServer **full remote file access**

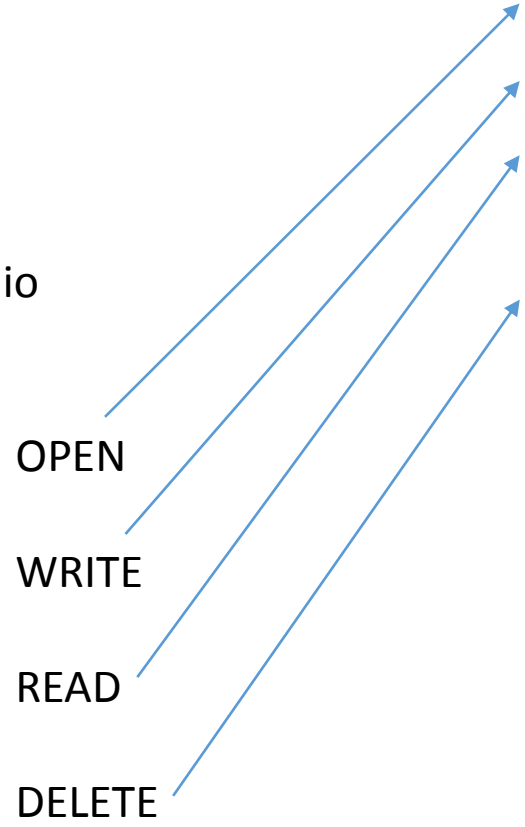
```
CEServer.exe is the remote agent server running on port 4322.

The protocol is constituited by an 8 bit opcode (from 0x01 to 0x39)
followed by the data.
Note that the commands are not handled for their real size but simply
as they are read from recv().

Through the following opcodes is possible to read, write, overwrite
and delete any file in the disks or shared folders accessible by the
software:

- 0x01 string:
  write mode with the NULL delimited name of the file to open, both
  absolute and relative paths supported
- 0x02 32bit data:
  the write operation where the opcode is followed by a 32bit number
  that specifies the amount of bytes to write and the data
- 0x04 string:
  read mode, same format as 0x01
- 0x05:
  request the reading of the file from the current position
- 0x0c string:
  creates a text file using the section/parameter/value syntax, that
  can be used to create bat files.
  the dot used below stands for the tab char (0x09)
    filename.section_name.parameter.value
- 0x15 string:
  remove the specified filename

Note that also some other opcodes perform file operations but the above
ones are the most important and with direct access to the files.
```



# Writing files in arbitrary and relative locations

Example:
CVE-2012-0232 - GE Intelligent Platforms Proficy Real-Time Information Portal Directory Traversal

## Effects

- Code Execution via commands executed at next boot/login
- Code Execution by overwrite specific executables
- Manipulate configurations by overwriting existing files

# Writing files in arbitrary and relative locations

Example:
CVE-2012-0232 - GE Intelligent Platforms Proficy Real-Time Information Portal Directory Traversal

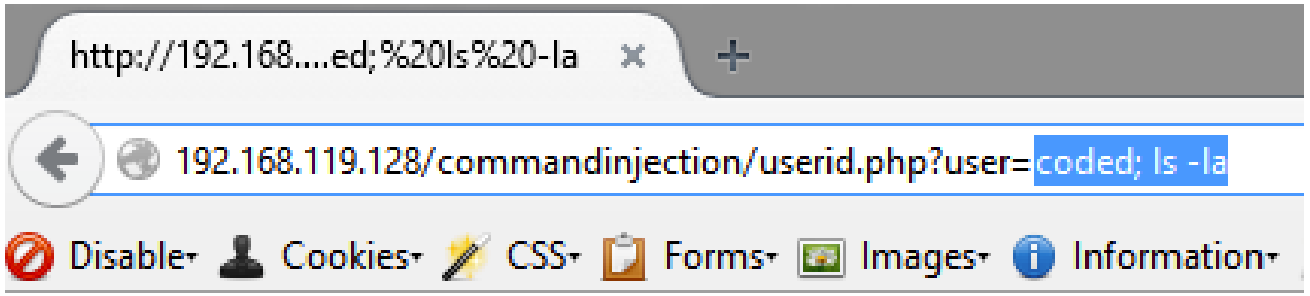
```
p = buff;
p += putxx(p, 1,    32);
p += putxx(p, 1,    32);
p += putss(p, "\\..\\..\\..\\..\\..\\..\\..\\..\\Documents and
Settings\\Administrator\\Start Menu\\Programs\\Startup\\test.bat");
p += putxx(p, 1025, 32);    // PORT
p += putxx(p, 1000, 32);    // PAUSE
p += putxx(p, 1,    32);    // SERVERCONF, boolean
p += putxx(p, 1,    32);    // number of strings, we need only one
p += putss(p,
   "\r\n"
   "\r\n"
   "@echo off\r\n"
   "net user test test /add\r\n"
   "net localgroup Administrators test /add\r\n"
   "net localgroup Administrator test /add\r\n"
   "net group \"Domain Admins\" test /add\r\n"
   //"del %0\r\n"
   "\r\n");
```

DESTINATION

DATA TO WRITE

# Arbitrary command execution and injection

Example:
CVE-2011-1566 – IGSS arbitrary command execution (directory traversal)




Example of this class of vulnerabilities

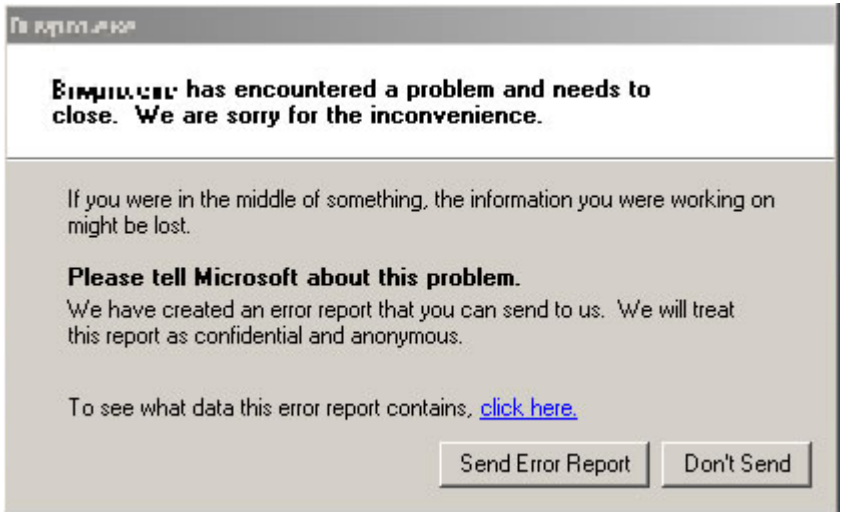
## Effects

- Code Execution via directory traversal
- Code Execution via shell injection in system()

Denial of Service

- NULL pointer
- Resource consumption (CPU and memory)
- Unexploitable memory corruption

Example:
CVE-2011-3489 - Rockwell Automation
RSLogix Overflow Vulnerability




Effects

- The service doesn’t work
- System unresponsive
- Other processes on the same machine may get affected

Web vulnerabilities

- SQL injection
- Local and Remote File Inclusion
- CSRF Cross-Site Request Forgery
- XSS Cross-site Scripting

Example:
CVE-2015-6461 – Schneider Electric
Modicon Remote File Inclusion


Example of this class of vulnerabilities

Effects

- Code execution
- Stolen information and database
- Authentication bypass

# Who reports security vulnerabilities in SCADA and industrial software & devices

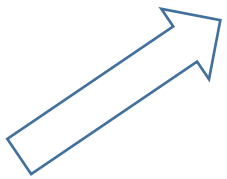
External researchers for fun or during the penetration testing of the products used by their clients, for example:

- Me till summer 2012
- Scada Strangelove project
- Many researchers via ICS-CERT / vendor
- Many researchers (publicly, not prior to vendor)

Vendors during the internal auditing of their products

0-days in the wild... rare event, for example Stuxnet

Cool, but…



Finding the software or the firmware

Finding the hardware devices

Configuring the products

Finding updates & patches

Is it a bug or a feature?!?

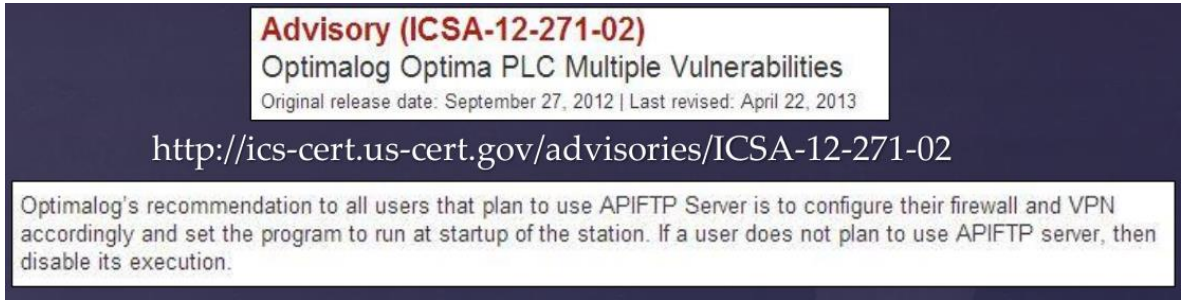
Possible vendor legal actions

# Patching SCADA and PLC vulnerabilities

The time required by the vendors to fix a vulnerability, testing the patch and releasing it is very long.
A 0-day may be fixed after various months.
And the situation is similar also for the vulnerabilities reported directly to the vendor *(coordinated disclosure)*

PDF: [Securing ICS Applications When Vendors Refuse Or Are Slow To Produce a Security Patch]

| Advisory Name: | Released: | Fixed*: | |
|---|---|---|---|
| winlog_1 | 12 jan 2011 -> 13 jan 2011 | +0 | |
| kingview 1 | 09 nov 2011 -> 22 dec 2011 | +1 | |
| abb_1 | 10 oct 2011 -> 22 feb 2012 | +4 | |
| indusoft_* | 27 apr 2011 -> 16 nov 2011 | +7 | |
| ifix_1 | 06 feb 2011 -> 07 nov 2011 | +9 | > 3 month |
| rtip_1 | 17 oct 2011 -> 22 aug 2012 | +10 | |
| ifix_2 | 17 oct 2011 -> 03 aug 2012 | +10 | |




Sometimes there is not even a patch and the vendor releases a “recommendation” for limiting the usage and access to the vulnerable component!

Sometimes the patches are not applied by the customers because not aware of the issues or to avoid downtimes and possible problems after patching… if it works why taking risks?

**Repository of Industrial Security Incidents (RISI)**
www.risidata.com

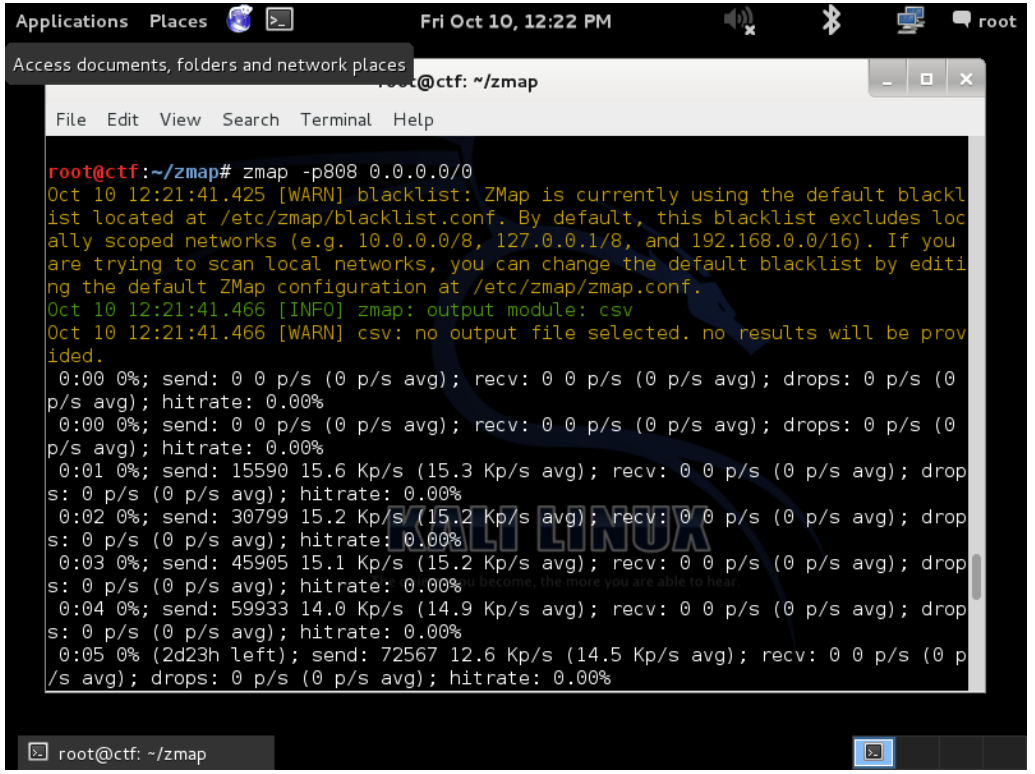
RISI — The Database | About | Contact

| Title | Year | Industry Type | Country | Brief |
|---|---|---|---|---|
| Page 1 of 9 pages 1 2 3 > Last › | | | | |
| German Steel Mill Cyber Attack | 2014 | Metals | Germany | |
| Russian-Based Dragonfly Group Attacks Energy Industry | 2014 | Power and Utilities | United States | |
| Public utility compromised after brute-force hack attack, says Homeland Security | 2014 | Power and Utilities | United States | |
| After 'Godzilla Attack!' U.S. warns about traffic-sign hackers | 2014 | Transportation | United States | |
| U-2 spy plane caused widespread shutdown of U.S. flights: report | 2014 | Transportation | United States | |
| Virus shuts down county highway department network | 2013 | Transportation | United States | |
| Signal problems cause train delays | 2013 | Transportation | United States | |
| Computer Glitch Leads to Shutdown of Nuclear Reactor | 2012 | Power and Utilities | United States | |
| U. S. Power Plant Infected With Malware | 2012 | Power and Utilities | United States | |
| U. S. Electric Utility Virus Infection | 2012 | Power and Utilities | United States | |
| Software Manufacturing Company Firewall Breach | 2012 | General Manufacturing | Canada | |
| Shamoon virus knocks out computers at Qatari gas firm RasGas | 2012 | Petroleum | Qatar | |
| Computer Virus Targets Saudi Arabian Oil Company | 2012 | Petroleum | Saudi Arabia | |
| Computer Glitch Causes Roller Coaster Malfunction | 2012 | Other | United States | |
| Computer Malfunction Causes Train Delays | 2012 | Transportation | United States | |
| Trains Shut Down Due to Computer Malfunction | 2012 | Transportation | United States | |
| Cascade of Computer Crashes Causes Metro System Shutdown | 2012 | Transportation | United States | |

Usual causes:

- **Accidental issues and failures**
- Angry employees
- General virus attacks
- Targeted cyber attacks
- Phishing

# Many infrastructures are reachable from the Internet

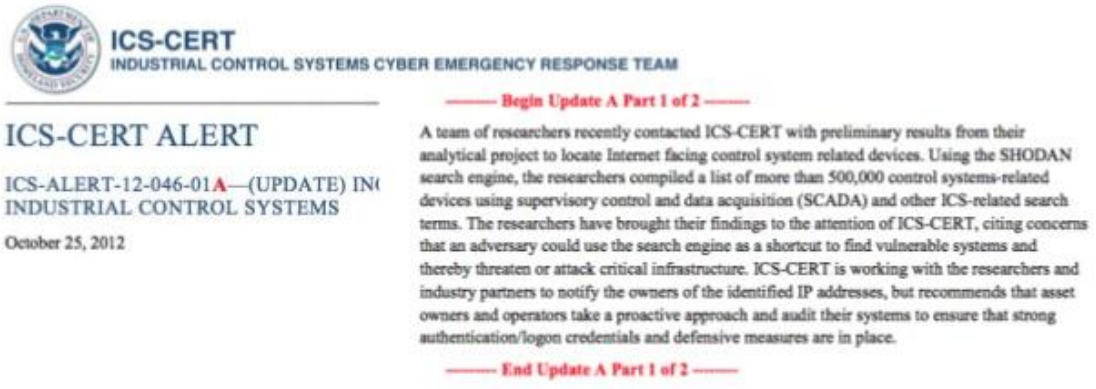




Shodan and manual scanning of selected IP ranges to spot easy-to-crack/open VNC sessions and SCADA products online

# Many infrastructures are reachable from the Internet
# Project SHINE

## Project SHINE – ICS/SCADA

- Project SHINE: **SH**odan **IN**telligence **E**xtraction
  - Bob Radvanovsky & Jake Brodsky  infracritical / scadasec
    - I provide research support, search terms, etc.
  - Daily search feed to ICS-CERT
  - 1,000,000 control systems discovered, 2K new each day



ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ALERT

ICS-ALERT-12-046-01A—(UPDATE) IN(
INDUSTRIAL CONTROL SYSTEMS

October 25, 2012

——— Begin Update A Part 1 of 2 ———

A team of researchers recently contacted ICS-CERT with preliminary results from their analytical project to locate Internet facing control system related devices. Using the SHODAN search engine, the researchers compiled a list of more than 500,000 control systems-related devices using supervisory control and data acquisition (SCADA) and other ICS-related search terms. The researchers have brought their findings to the attention of ICS-CERT, citing concerns that an adversary could use the search engine as a shortcut to find vulnerable systems and thereby threaten or attack critical infrastructure. ICS-CERT is working with the researchers and industry partners to notify the owners of the identified IP addresses, but recommends that asset owners and operators take a proactive approach and audit their systems to ensure that strong authentication/logon credentials and defensive measures are in place.

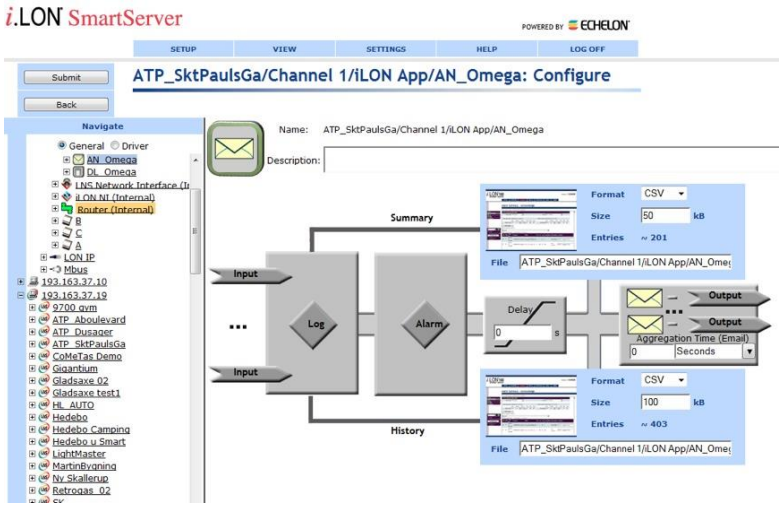
——— End Update A Part 1 of 2 ———

Attempt to use Shodan to spot industrial servers and devices through various queries.

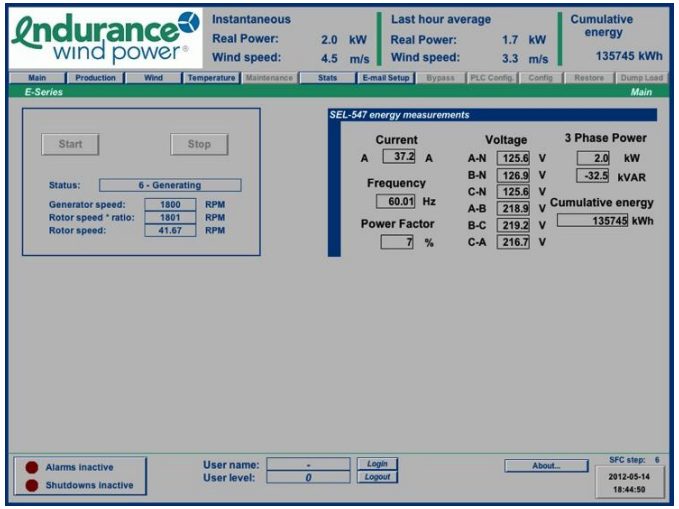
They claim to have found over 2 millions of devices between 2012 and 2014.

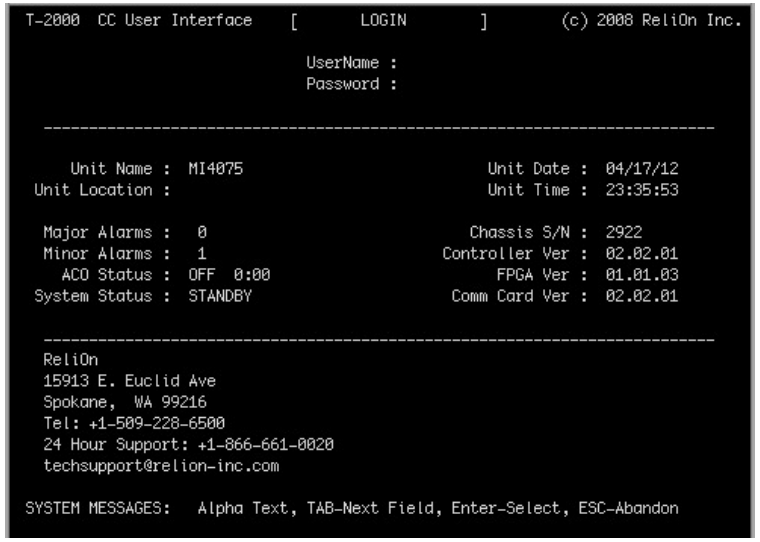
Some statistical results were released.

# Many infrastructures are reachable from the Internet
# Viss' results and Project SONAR





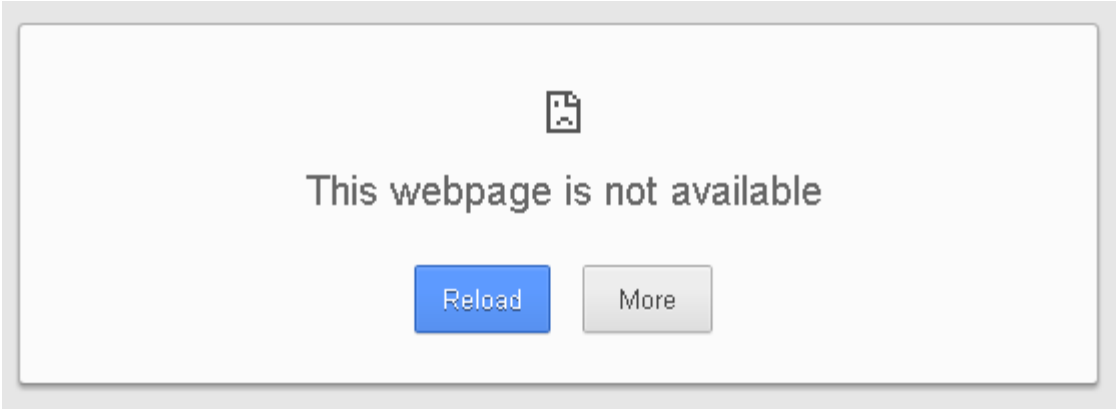



Dan Tentler ("Viss") used SHODAN to find systems meant to be private, but freely available on the Internet like webcams, VNC servers, SCADA systems and other industrial related results.

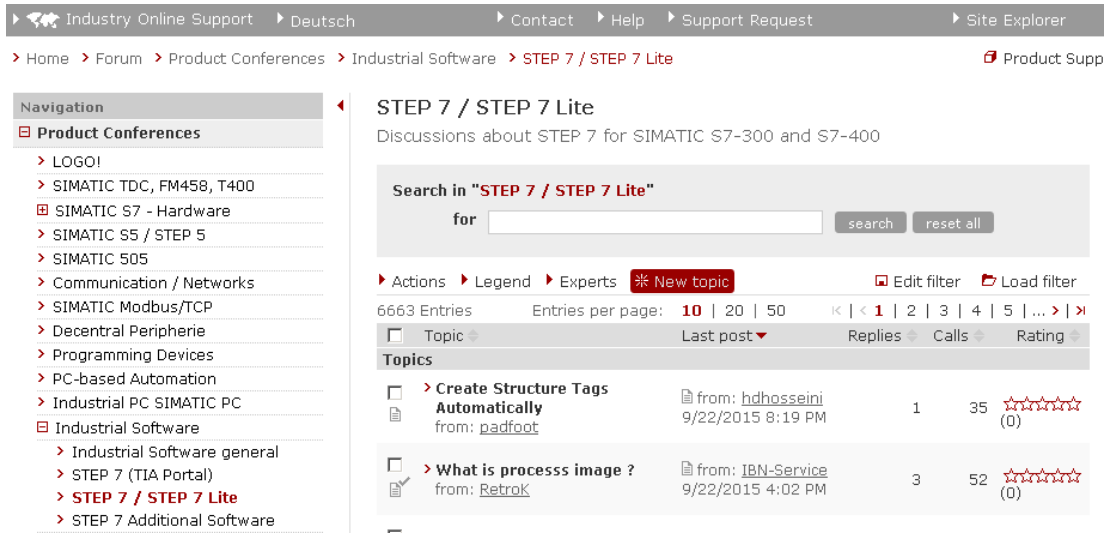
# What to do

1. No Internet access
2. Keep your systems updated
3. Strong and unrelated passwords
4. General network security *(limit/disable wi-fi, firewall, AV)*
5. Microsoft EMET *(The Enhanced Mitigation Experience Toolkit)*
6. Limit network access to the systems
7. Limit human access to the systems *(USB/keyboard)*
8. Stay informed

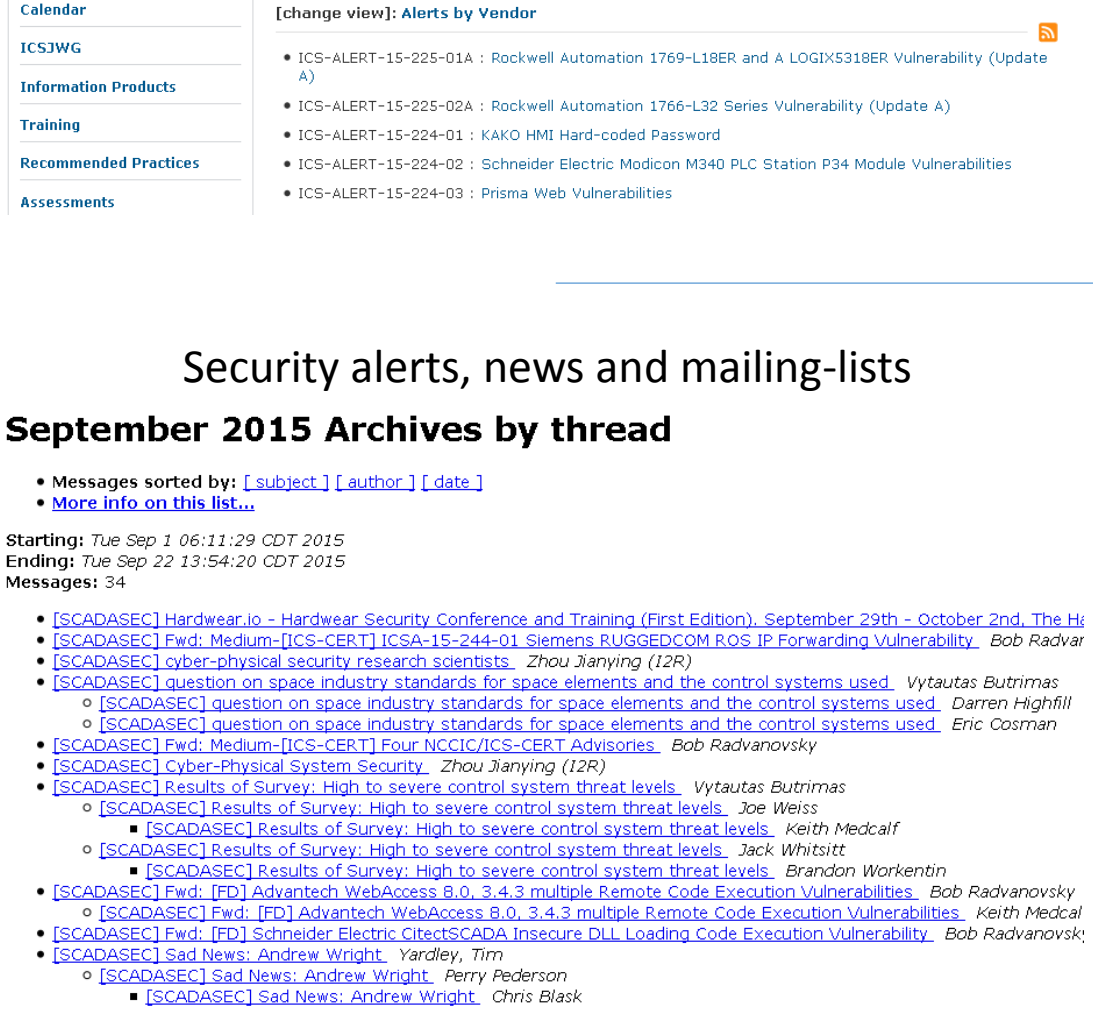


# ICS-CERT


# Official forums




# Security alerts, news and mailing-lists




# Unofficial forums