

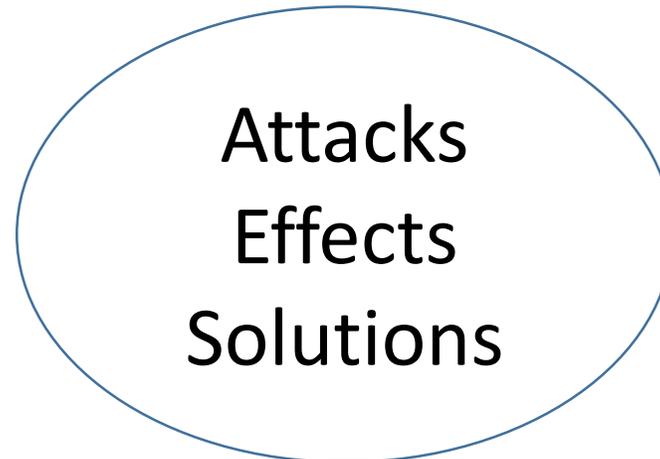
Architecture

Vulnerabilities

Attack Surface

Real Examples

Suggestions



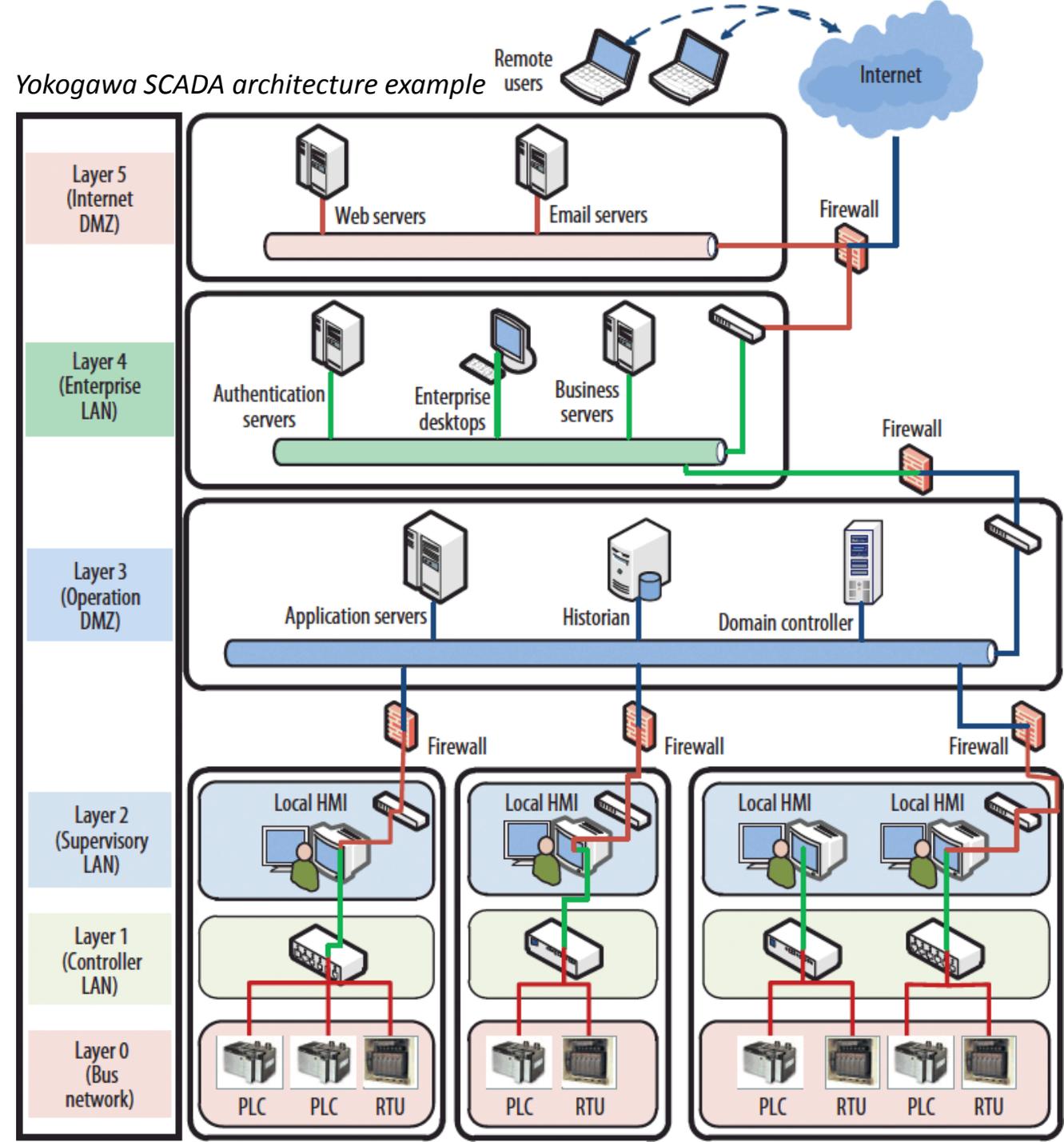
SCADA architecture

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

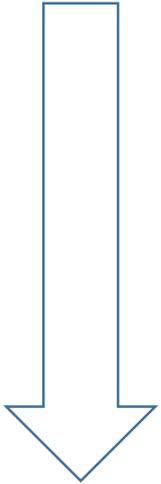
What's sure is that more devices will be connected via TCP/IP, and so, it's more easy to get reached by possible attackers.

Yokogawa SCADA architecture example

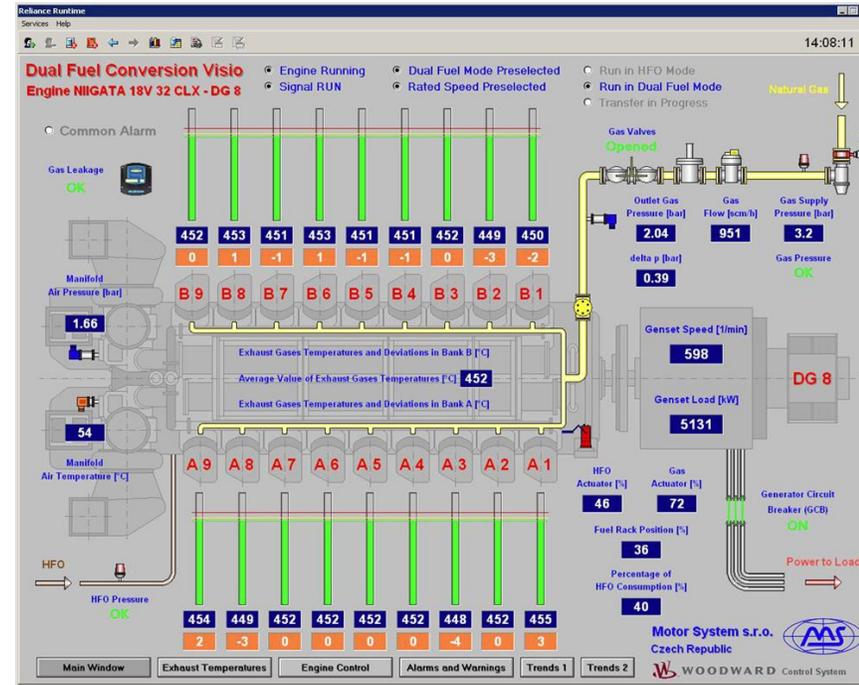


TARGETS

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

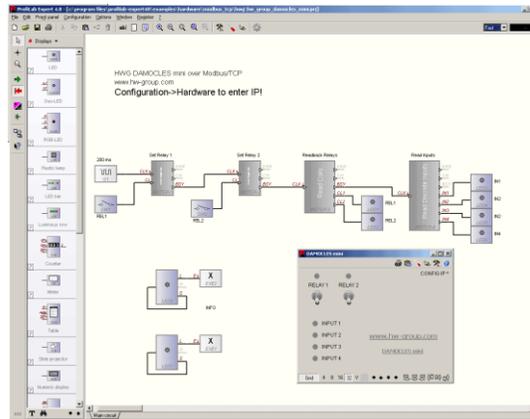


HMI/SCADA ATTACK SURFACE

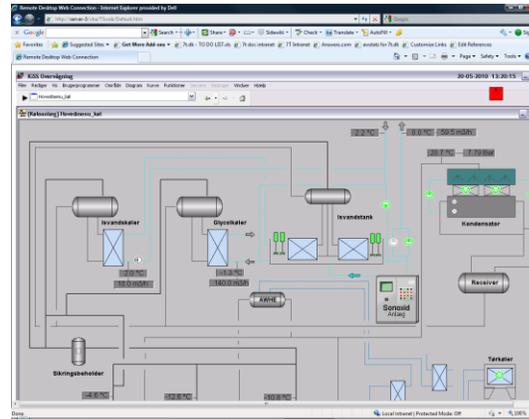
Server-side vulnerabilities through TCP and UDP open ports



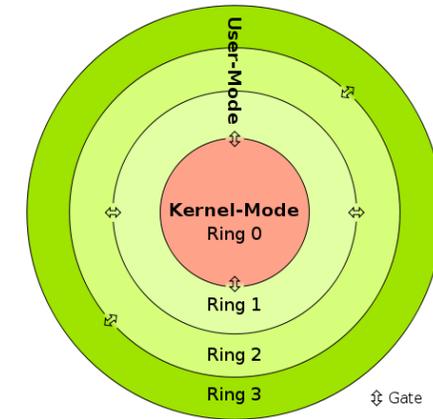
Handling of project files and other files with registered extensions



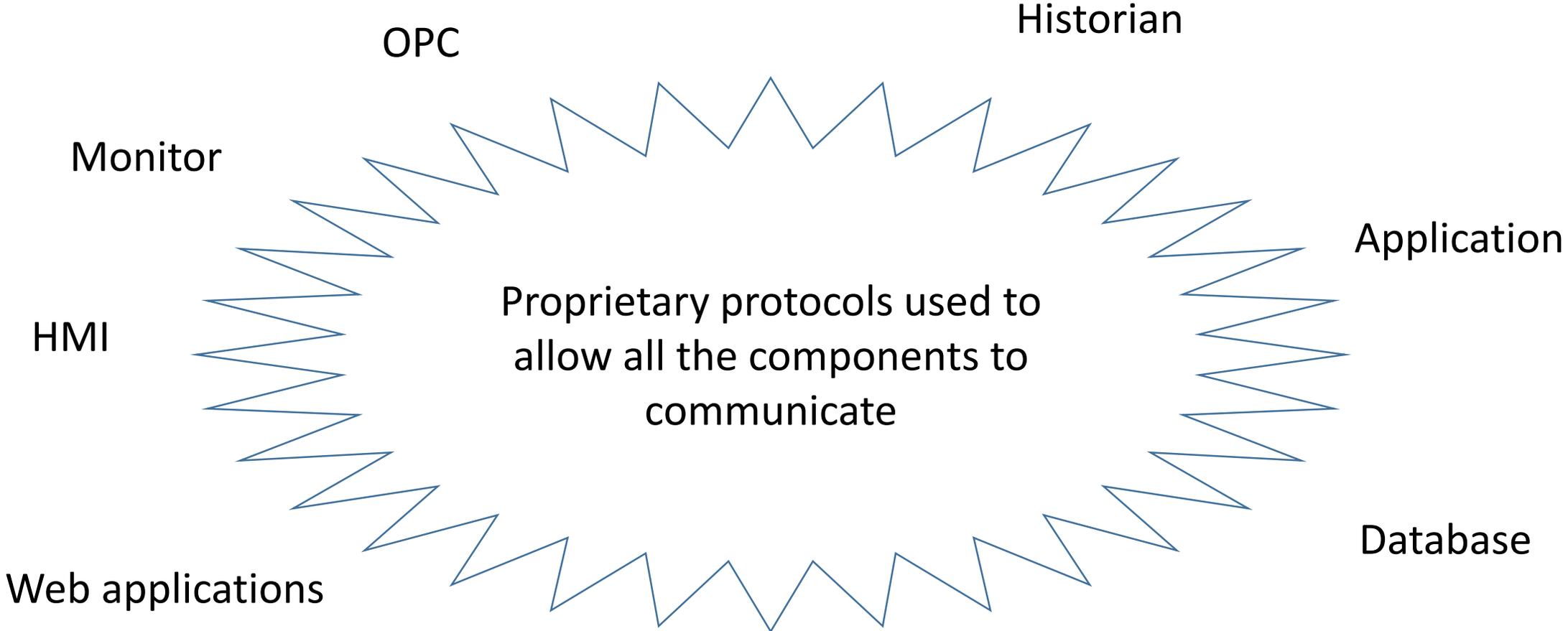
Client-side vulnerabilities through the integration in web browsers: *ActiveX* and *URL protocols*



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.

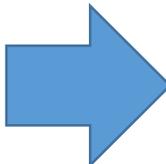
Mitigation

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, maintenance 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-15-181-02)

SMA Solar Technology AG Sunny WebBox Hard-coded Account Vulnerability

Original release date: September 03, 2015

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-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

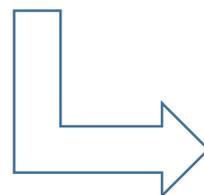
Original release date: July 24, 2014

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



Кибер	Добавлено	Пт Апр 11, 2008 19:27	Заголовок со
Новый писатель	login='WinCCConnect' password='2WSXcder' login='WinCCAdmin' password='2WSXcde.'		
Зарегистрирован			
22.10.2007			
Сообщения: 14			

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 of SQL server its set at mixed (sql server and windows)..

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

Note: I am working with wincc of PCS7 environment

Thanks in advance..
Duncan.

2006



Cyber
Новый писатель
Добавлено: Пт Апр 11, 2008 19:27
Заголовок сообщения:
`login='WinCCConnect' password='2WSXcder'
login='WinCCAdmin' password='2WSXcde.'`
Зарегистрирован:
22.10.2007
Сообщения: 14

4/15/2008 9:31 PM
Rate ☆☆☆☆☆ (0)

[Dec](#)

Gold Expert
Joined: 5/19/2006
Last visit: 6/10/2015

Hey Cyber,
Are we suppose to congratulate you for cracking those passwords?
Those accounts/passwords were mainly designed to ensure the use of a genuine MS-SQL setup from WinCC Delivery CD/DVD and not a customer purchased version of MSSQL (see EULA).

Dec

2008



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.

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.

2012



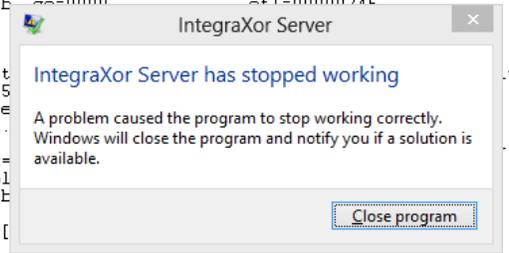
Memory corruption vulnerabilities

- 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)

Effects

- Code Execution
- Denial of Service in case of failure

```
ModLoad: 64890000 648b9000 C:\Windows\System32\ScrRun.dll
ModLoad: 6ad80000 6ad99000 C:\Windows\system32\wbem\wmiutils.dll
ModLoad: 6ada0000 6adb0000 C:\Windows\system32\wbem\wbemsvc.dll
ModLoad: 6adb0000 6ae72000 C:\Windows\system32\wbem\fastprox.dll
(fc8.334): Break instruction exception - code 80000003 (first chance)
*** ERROR: Symbol file could not be found. Defaulted to export symbols for C:\Windows\SYSTEM32\nt
*** ERROR: Symbol file could not be found. Defaulted to export symbols for C:\Windows\system32\KE
eax=7f533000 ebx=00000000 ecx=00000000 edx=7745a7c3 esi=00000000 edi=00000000
eip=77381244 esp=0fb2f940 ebp=0fb2f96c iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246
ntdll!DbgBreakPoint:
77381244 cc                int     3
0:088> g
ig > 14:30.111 > [socket] select failed with error 0: The operation completed successfully.
(fc8.b48): Access violation - code c0000005 (!!! second chance !!!)
First chance exceptions are reported before this exception may be expected and handled.
*** ERROR: Symbol file could not be found. Defaulted to export symbols for C:\Windows\system32\KE
eax=0b7ae180 ebx=00000008 ecx=00000061 edx=76bb682d eip=76bb682d esp=0b7ae0f4 ebp=0b7ae11c iopl=0
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010202
KERNEL32!lstrcpyW+0x1b:
76bb682d 66890a          mov     word ptr [eax], 0
0:023> d edx-10
0b7afff0 61 00 61 00 61 00 61 00-61 00 61 00 61 00 61 00  a.a.a.a.a.a.a.a
0b7b0000 ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ??  ????????????????
0b7b0010 ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ??  ????????????????
0b7b0020 ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ??  ????????????????
0b7b0030 ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ??  ????????????????
0b7b0040 ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ??  ????????????????
0b7b0050 ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ??  ????????????????
0b7b0060 ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ??  ????????????????
0:023> gm
ig > 14:44.051 > [socket] select failed with error 0: The operation completed successfully.
(fc8.b48): Access violation - code c0000005 (!!! second chance !!!)
eax=0b7ae180 ebx=00000008 ecx=00000061 edx=0b7b0000 esi=0be33ed8 edi=0be32058
eip=76bb682d esp=0b7ae0f4 ebp=0b7ae11c iopl=0         nv up ei pl nz na po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010202
KERNEL32!lstrcpyW+0x1b:
76bb682d 66890a          mov     word ptr [eax], 0
```



Example:

[CVE-2011-5007](#) – 3S CodeSys buffer-overflow

...
Why is it interesting?

Memory corruption vulnerabilities

	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

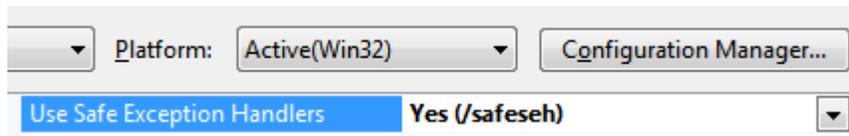
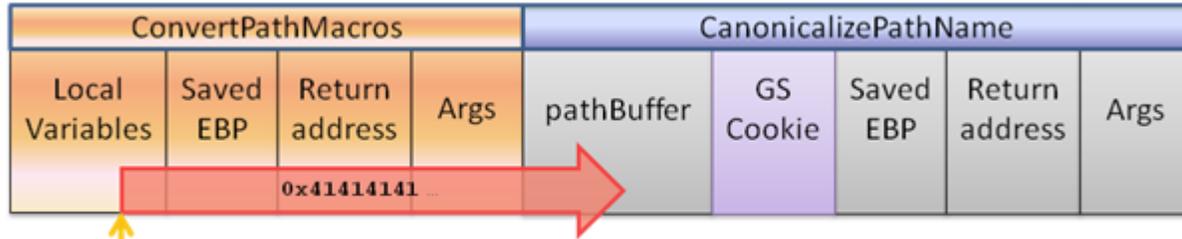
...

Why is it interesting?

Because the issue was in a library used also on ABB PLCs!

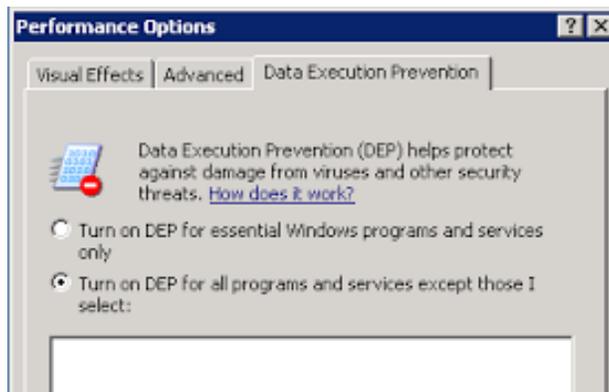
(ICSA-12-006-01 and ICSA-12-320-01)

Stack protections and secured exception handlers



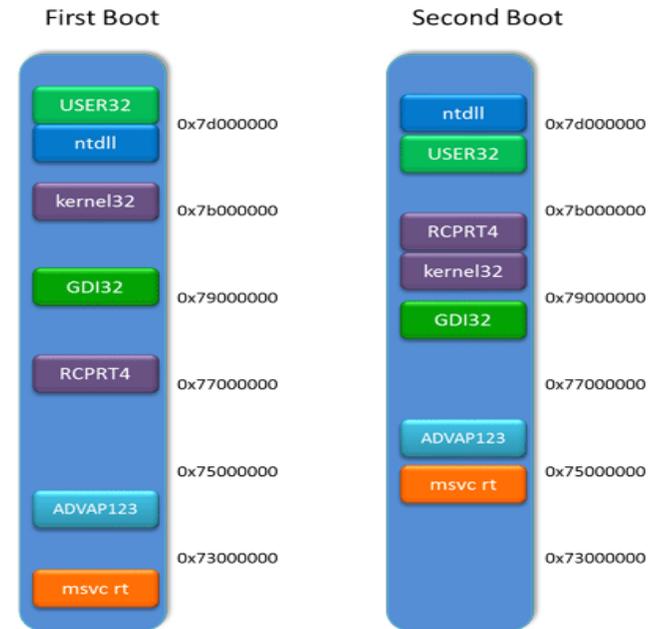
DEP

Data Execution Prevention



ASLR

Address Space Layout Randomization



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 CServer full remote file access



Effects

- Stealing information and sensitive data

Information disclosure vulnerabilities

[CVE-2011-4051](#) – Indusoft WebStudio CEServer full remote file access

OPEN

WRITE

READ

DELETE

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

The protocol is constituted 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



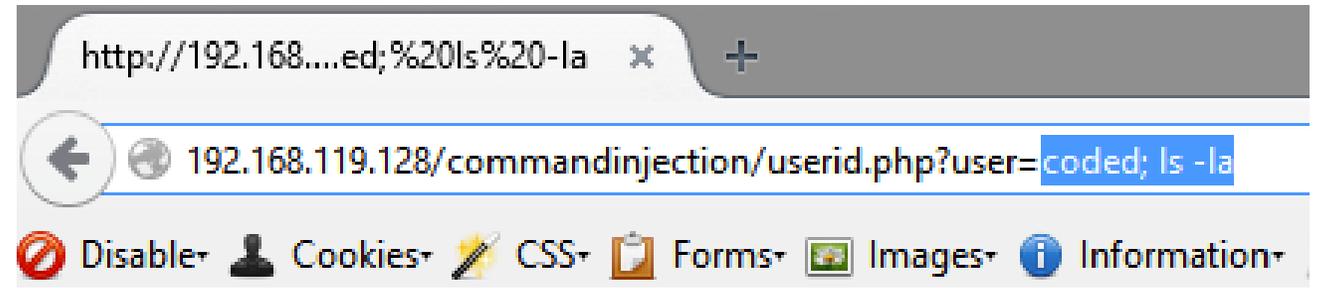
Effects

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

Arbitrary command execution and injection

Example:

[CVE-2011-1566](#) – IGSS arbitrary command execution (directory traversal)



Example of this class of vulnerabilities

Effects

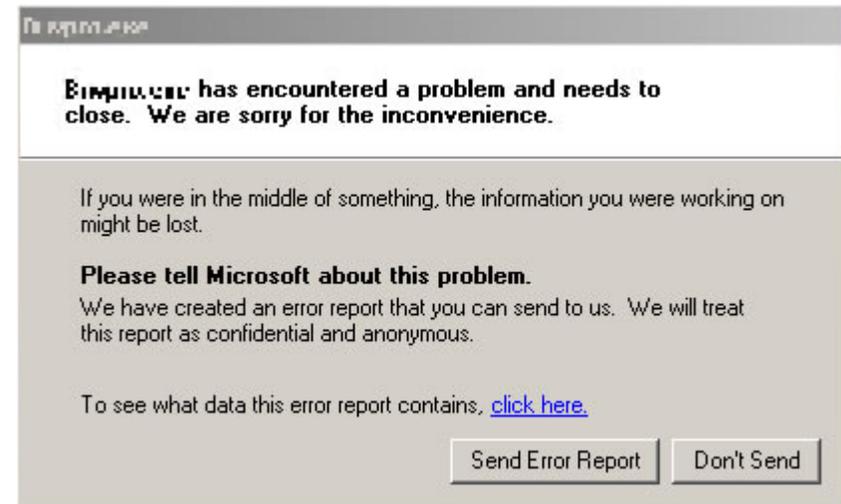
- Code Execution via directory traversal
- Code Execution via shell injection in system()

Denial of Service

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

Example:

[CVE-2011-3489](#) - Rockwell Automation
RSLogix Overflow Vulnerability



Effects

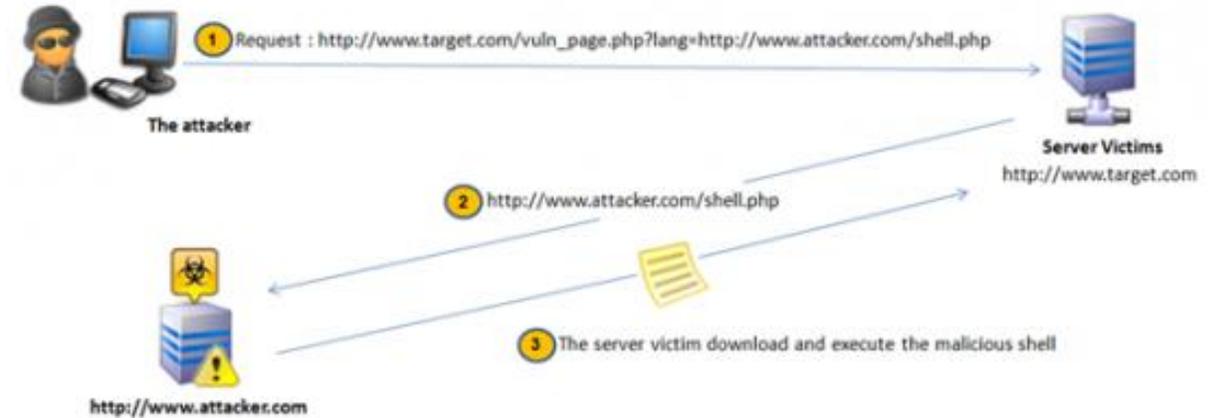
- The service doesn't work
- System unresponsive
- Other processes on the same machine may get affected

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

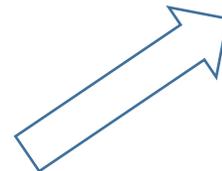
External researchers for fun or during the penetration testing of the products used by their clients, for example:

- 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
rtip_1	17 oct 2011	-> 22 aug 2012	+10
ifix_2	17 oct 2011	-> 03 aug 2012	+10

> 3 month

Advisory (ICSA-12-271-02)

Optimalog Optima PLC Multiple Vulnerabilities

Original release date: September 27, 2012 | Last revised: April 22, 2013

<http://ics-cert.us-cert.gov/advisories/ICSA-12-271-02>

Optimalog's recommendation to all users that plan to use APIFTP Server is to configure their firewall and VPN accordingly and set the program to run at startup of the station. If a user does not plan to use APIFTP server, then disable its execution.

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

Usual causes:

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

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	🔍			

Many infrastructures are reachable from the Internet



SHODAN

Filter by Country

Filter by Service

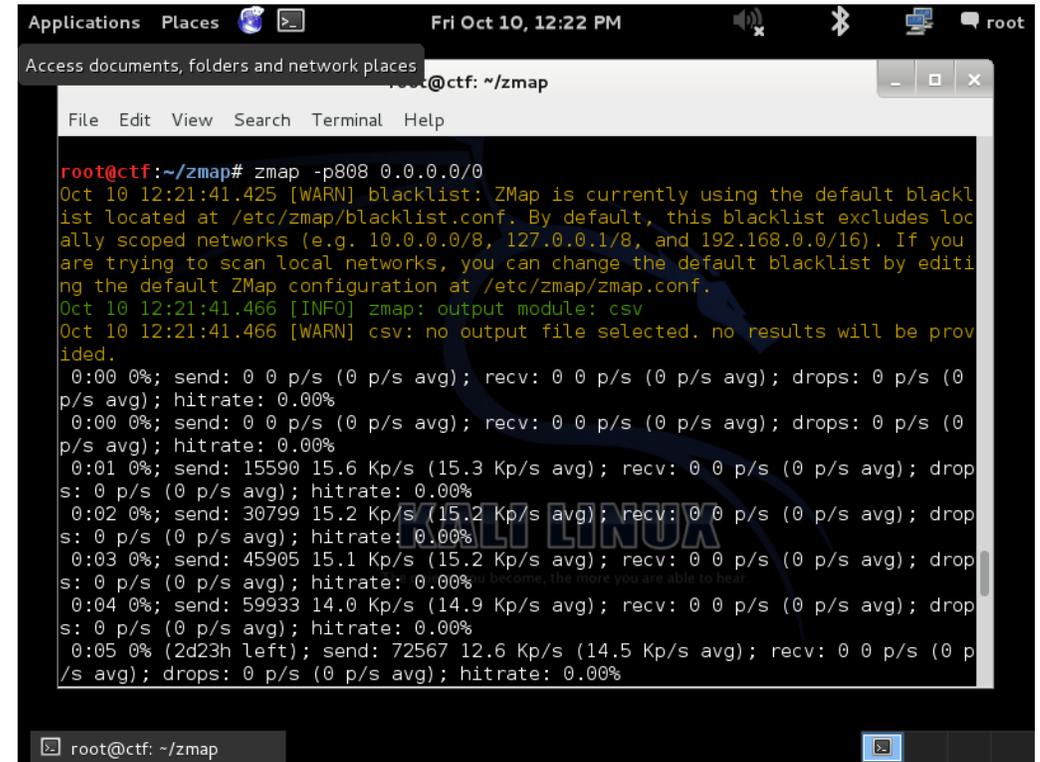
- HTTP (80)
- FTP (21)
- SSH (22)
- SNMP (161)
- SIP (5060)

EXPOSE ONLINE DEVICES.

WEBCAMS. ROUTERS.
POWER PLANTS. IPHONES. WIND TURBINES.
REFRIGERATORS. VOIP PHONES.

[TAKE A TOUR](#) [FREE SIGN UP](#)

Popular Search Queries: iPads - iPads. Think different. Think no security.



```
root@ctf: ~/zmap
File Edit View Search Terminal Help

root@ctf:~/zmap# zmap -p808 0.0.0.0/0
Oct 10 12:21:41.425 [WARN] blacklist: ZMap is currently using the default blacklist located at /etc/zmap/blacklist.conf. By default, this blacklist excludes locally scoped networks (e.g. 10.0.0.0/8, 127.0.0.1/8, and 192.168.0.0/16). If you are trying to scan local networks, you can change the default blacklist by editing the default ZMap configuration at /etc/zmap/zmap.conf.
Oct 10 12:21:41.466 [INFO] zmap: output module: csv
Oct 10 12:21:41.466 [WARN] csv: no output file selected. no results will be provided.
0:00 0%; send: 0 0 p/s (0 p/s avg); recv: 0 0 p/s (0 p/s avg); drops: 0 p/s (0 p/s avg); hitrate: 0.00%
0:00 0%; send: 0 0 p/s (0 p/s avg); recv: 0 0 p/s (0 p/s avg); drops: 0 p/s (0 p/s avg); hitrate: 0.00%
0:01 0%; send: 15590 15.6 Kp/s (15.3 Kp/s avg); recv: 0 0 p/s (0 p/s avg); drops: 0 p/s (0 p/s avg); hitrate: 0.00%
0:02 0%; send: 30799 15.2 Kp/s (15.2 Kp/s avg); recv: 0 0 p/s (0 p/s avg); drops: 0 p/s (0 p/s avg); hitrate: 0.00%
0:03 0%; send: 45905 15.1 Kp/s (15.2 Kp/s avg); recv: 0 0 p/s (0 p/s avg); drops: 0 p/s (0 p/s avg); hitrate: 0.00%
0:04 0%; send: 59933 14.0 Kp/s (14.9 Kp/s avg); recv: 0 0 p/s (0 p/s avg); drops: 0 p/s (0 p/s avg); hitrate: 0.00%
0:05 0% (2d23h left); send: 72567 12.6 Kp/s (14.5 Kp/s avg); recv: 0 0 p/s (0 p/s avg); drops: 0 p/s (0 p/s avg); hitrate: 0.00%
```

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

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.



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 —————

Many infrastructures are reachable from the Internet

Viss' results and Project SONAR

iLON SmartServer POWERED BY ECHOLON

ATP_SktPaulsGa/Channel 1/iLON App/AN_Omega: Configure

Name: ATP_SktPaulsGa/Channel 1/iLON App/AN_Omega

Description:

Summary: File [ATP_SktPaulsGa/Channel 1/iLON App/AN_Omega], Format CSV, Size 50 kb, Entries ~ 201

History: File [ATP_SktPaulsGa/Channel 1/iLON App/AN_Omega], Format CSV, Size 100 kb, Entries ~ 403

Flow: Input → Log → Alarm → History → Output (Email)

ACUM GAUGES (Torr)

PRESSURE (Psta)

TEMPERATURE (deg. K)

SYSTEM STATUS

AUTO FILL MODE

BAKEOUT MODE

LEVEL CONTROLS

Endurance wind power

Instantaneous Real Power: 2.0 kW, Wind speed: 4.5 m/s

Last hour average Real Power: 1.7 kW, Wind speed: 3.3 m/s

Cumulative energy: 135745 kWh

SEL-547 energy measurements

Current	Voltage	3 Phase Power
A 37.2 A	A-N 125.6 V	2.0 kW
	B-N 126.9 V	-32.5 kVAR
	C-N 125.6 V	
Frequency 60.01 Hz	A-B 218.9 V	Cumulative energy 135745 kWh
Power Factor 7 %	B-C 219.2 V	
	C-A 216.7 V	

```

T-2000 CC User Interface [ LOGIN ] (c) 2008 ReliOn Inc.

UserName :
Password :

-----
Unit Name : MI4075          Unit Date : 04/17/12
Unit Location :           Unit Time : 23:35:53

Major Alarms : 0          Chassis S/N : 2922
Minor Alarms : 1          Controller Ver : 02.02.01
ACD Status : OFF 0:00     FPGA Ver : 01.01.03
System Status : STANDBY   Comm Card Ver : 02.02.01

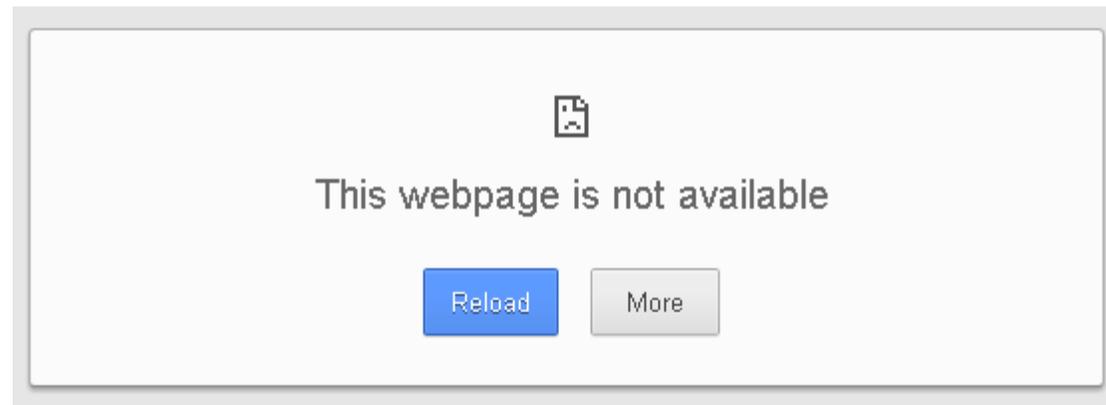
-----
ReliOn
15913 E. Euclid Ave
Spokane, WA 99216
Tel: +1-509-228-6500
24 Hour Support: +1-866-661-0020
techsupport@reli-on.com

SYSTEM MESSAGES: Alpha Text, TAB-Next Field, Enter-Select, ESC-Abandon
    
```

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



- HOME
- ABOUT
- ICSJWG
- INFORMATION PRODUCTS
- TRAINING
- FAQ

- Control Systems
- Home
- Calendar
- ICSJWG
- Information Products
- Training
- Recommended Practices
- Assessments

ICS-CERT Alerts

An ICS-CERT Alert is intended to provide timely notification to critical infrastructure owners and operators concerning threats or activity with the potential to impact critical infrastructure computing networks.

[change view]: Alerts by Vendor

- ICS-ALERT-15-225-01A : Rockwell Automation 1769-L18ER and A LOGIX5318ER Vulnerability (Update A)
- ICS-ALERT-15-225-02A : Rockwell Automation 1766-L32 Series Vulnerability (Update A)
- ICS-ALERT-15-224-01 : KAKO HMI Hard-coded Password
- ICS-ALERT-15-224-02 : Schneider Electric Modicon M340 PLC Station P34 Module Vulnerabilities
- ICS-ALERT-15-224-03 : Prisma Web Vulnerabilities

Security alerts, news and mailing-lists

September 2015 Archives by thread

- Messages sorted by: [subject] [author] [date]
- [More info on this list...](#)

Starting: Tue Sep 1 06:11:29 CDT 2015

Ending: Tue Sep 22 13:54:20 CDT 2015

Messages: 34

- [SCADASEC] [Hardware.io - Hardware Security Conference and Training \(First Edition\), September 29th - October 2nd, The H...](#)
- [SCADASEC] [Fwd: Medium-\[ICS-CERT\] ICSA-15-244-01 Siemens RUGGEDCOM ROS IP Forwarding Vulnerability](#) Bob Radvar
- [SCADASEC] [cyber-physical security research scientists](#) Zhou Jianying (12R)
- [SCADASEC] [question on space industry standards for space elements and the control systems used](#) Vytautas Butrimas
 - [SCADASEC] [question on space industry standards for space elements and the control systems used](#) Darren Highfill
 - [SCADASEC] [question on space industry standards for space elements and the control systems used](#) Eric Cosman
- [SCADASEC] [Fwd: Medium-\[ICS-CERT\] Four NCCIC/ICS-CERT Advisories](#) Bob Radvanovskij
- [SCADASEC] [Cyber-Physical System Security](#) Zhou Jianying (12R)
- [SCADASEC] [Results of Survey: High to severe control system threat levels](#) Vytautas Butrimas
 - [SCADASEC] [Results of Survey: High to severe control system threat levels](#) Joe Weiss
 - [SCADASEC] [Results of Survey: High to severe control system threat levels](#) Keith Medcalf
 - [SCADASEC] [Results of Survey: High to severe control system threat levels](#) Jack Whitsitt
 - [SCADASEC] [Results of Survey: High to severe control system threat levels](#) Brandon Workentin
- [SCADASEC] [Fwd: \[FD\] Advantech WebAccess 8.0, 3.4.3 multiple Remote Code Execution Vulnerabilities](#) Bob Radvanovskij
 - [SCADASEC] [Fwd: \[FD\] Advantech WebAccess 8.0, 3.4.3 multiple Remote Code Execution Vulnerabilities](#) Keith Medcalf
- [SCADASEC] [Fwd: \[FD\] Schneider Electric CitectSCADA Insecure DLL Loading Code Execution Vulnerability](#) Bob Radvanovskij
- [SCADASEC] [Sad News: Andrew Wright](#) Yardley, Tim
 - [SCADASEC] [Sad News: Andrew Wright](#) Perry Pederson
 - [SCADASEC] [Sad News: Andrew Wright](#) Chris Blask

Official forums

- Industry Online Support
 - Deutsch
 - Contact
 - Help
 - Support Request
 - Site Explorer
- Home > Forum > Product Conferences > Industrial Software > STEP 7 / STEP 7 Lite

- Navigation
- Product Conferences
 - LOGO!
 - SIMATIC TDC, FM458, T400
 - SIMATIC S7 - Hardware
 - SIMATIC S5 / STEP 5
 - SIMATIC 505
 - Communication / Networks
 - SIMATIC Modbus/TCP
 - Decentral Peripherie
 - Programming Devices
 - PC-based Automation
 - Industrial PC SIMATIC PC
 - Industrial Software
 - Industrial Software general
 - STEP 7 (TIA Portal)
 - STEP 7 / STEP 7 Lite
 - STEP 7 Additional Software

STEP 7 / STEP 7 Lite

Discussions about STEP 7 for SIMATIC S7-300 and S7-400

Search in "STEP 7 / STEP 7 Lite" for

6663 Entries Entries per page: 10 | 20 | 50 << | < 1 | 2 | 3 | 4 | 5 | ... > | >>

Topic	Last post	Replies	Calls	Rating
Create Structure Tags Automatically from: padfoot	from: hdsosseini 9/22/2015 8:19 PM	1	35	☆☆☆☆☆ (0)
What is process image ? from: RetroK	from: IBN-Service 9/22/2015 4:02 PM	3	52	☆☆☆☆☆ (0)

Unofficial forums

plcforum.uz.ua
International PLC Forum

Login Register

It is currently Tue Sep 22, 2015 10:46 pm

[View unanswered posts](#) | [View active topics](#)

[Board index](#) » [International User Forum](#) All times are UTC + 3 hours

Forum rules

[Please click here to view the forum rules](#)

Forum	Topics	Posts	Last post
SIMATIC Automation			
SIMATIC system SIMATIC S7-200/300/400, Step7, PCS7, CFC, SFC, PDM, PLCSIM, SCL, Graph, SPS-VISU S5/S7, IBHsoftec, LOGO ...	2714	9200	Tue Sep 22, 2015 11:45 am ppp →
Utilites for Simatic PLC Utilites for Simatic Automation	57	248	Thu Sep 10, 2015 2:42 am bialy_madrid →
Siemens SIMATIC HMI			