

SCADA STRANGELOVE



SCADA.SL



# ATTACKING SCADA SYSTEMS: STORY OF SCADASTRANGELOVE

\*All pictures are taken from Dr Strangelove movie and other Internets

Sergey Gordeychik  
Aleksandr Timorin  
Gleb Gritsai

# whoami

Aleksandr Timorin lifecycle:

- Studied mathematics (OMG!)
- Python developer
- Penetration tester
- ICS security researcher:
  - Industrial protocols fan and 0-day PLC hunter
  - SCADAStrangeLove team member



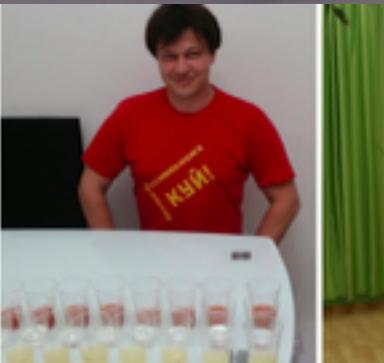
atimorin

atimorin@protonmail.ch

# AGENDA

- WWW: **who** are we, **why** are we and **what** are we for ?
- Milestone
- Projects:
  - Past
  - Present
  - Future
- Results

# WWW



# @scadasl

- Group of security researchers focused on ICS/SCADA

Alexander Timorin

Dmitry Serebryannikov

Sergey Drozdov

Alexander Tlyapov

Dmitry Sklyarov

Sergey Gordeychik

Alexander Zaitsev

Evgeny Ermakov

Sergey Scherbel

Alexey Osipov

Gleb Gritsai

Timur Yunusov

Andrey Medov

Ilya Karpov

Valentin Shilnenkov

Artem Chaykin

Ivan Poliyanchuk

Vladimir Kochetkov

Denis Baranov

Kirill Nesterov

Vyacheslav Egoshin

Dmitry Efanov

Roman Ilin

Yuri Goltsev

Dmitry Nagibin

Sergey Bobrov

Yuriy Dyachenko

---

to **save** Humanity **from** industrial **disaster**  
and to **keep** Purity Of Essence

# WWW

- We work for community and as community



# WWW

Since Stuxnet (2010) ICS industry especially security has been warned.



in-destroya

# WWW

- ICS is everywhere
- Old technologies without classic and modern security principles
- ICS networks “isolated”, but connected to other nets, other nets connected to Internet
- Sometimes (shodan/censys/zmap/masscan proved) ICS devices connected to the Internet directly
- Hacking ICS without money does not attract evil guy
- Engineers tend to say “this works for a long period of time!  
Don’t touch it!”

# WWW

- But reality shows us that evil guys touch them and ICS so tender
- We was worried about it.
- We didn't accept this approach.
- We decided to change situation.
- Then SCADASTRANGELOVE was born



WWW

Peace is our profession!



# WWW

- As a group of researchers we work in different companies
- Not only one company with private atmosphere
- Everybody can be a member



www

Members have their own projects but still contributing to long-term  
projects #SCADAPASS and #SCADASOS

RT @mmrupp: Another wind farm in Europe with a trivial mistake. It will be added to #SCADASOS tag after fixing.



# WWW

- We regularly give a talks worldwide in security conferences: CCC, Power of Community, CodeBlue, PacSec, PHDays, Zeronights, Confidence, Hack.lu ...
- We show and share our results with community
- We share researches of our projects
- We share toolkits, scripts, dorks, analytics and statistics

# Milestone

- 2012: only 4 members
- From 2013 to 2016: over 30 members
- Over 100 0-dayz
- Tons of vulnerabilities: binary, web, default credentials and so on
- Different industries: from transportation to renewable energy

# Milestone

## Vulnerabilities:

- Memory errors
- Cryptofails
- Web
- Special “features” (aka backdoors)
- Default and hardcoded credentials
- Industrial protocols
- Fun but non-profit

# Milestone

## Vulnerabilities:

- Siemens
- General electric
- Schneider electric
- Yokogawa
- Honeywell
- Abb
- Advantech
- etc

# Milestone

## Vulnerabilities:

- Server/client scada software
- PLC, HMI, RTU
- Protective relays, actuators, converters
- Smart meters, data concentrators
- Network switches, gateways
- Gsm/gprs modems
- etc

# Input validation: Buffer overflow

- Honeywell EPKS, CVE-2014-9189

```
len = 2 * *((_WORD *)buffer3);  
_=r((char *)String, buffer3 + 2, len, 0);
```

```
uchar_t String[80]; // [sp+16Ch] [bp-134h]@1
```

```
signed int __cdecl [redacted](char *dst, char *src, int inSize, int ah)
{
    signed int result; // eax@2
    int v5; // edx@3
    char *ptr; // ecx@4
    unsigned int v8; // eax@5

    if ([redacted] == 0) // sub_48[0]
    {
        result = -1;
    }
    else
    {
        v5 = 0;
        if ( inSize > 0 )
        {
            ptr = src;
            do
            {
                LOBYTE(v8) = *(&byte_58[4 * (unsigned __int8)*ptr] + *ptr + v5);
                ptr[dst - src] = v8;
                if ( ah )
                    v8 = (unsigned __int8)*ptr;
                else
                    v8 = (unsigned __int8)v8;
                v5 = (signed int)v8 % 5;
                ++ptr;
                --inSize;
            }
            while ( inSize );
        }
    }
}
```

# Input validation: Buffer overflow (2)

- Honeywell EPKS, CVE-2014-9187

```
buffer3 = (char *)U[...].alloc(2 * a5);
IF ( !buffer3 )
{
    unixmsg(
        188,
        10,
        OFF_52E914,
        (int)"384",
        "...", // [REDACTED] %d bytes of memory",
        2 * a5);
    goto LABEL_199;
}
memset(buffer3, 0, 2 * a5);
v35 = re[...].timeout(Arqlist, buffer3, *(int *)&buf[16], 10);
```

# Input validation: God help us all

- cb is a buffer size

```
if ( cb >= v170 )
{
    v112 = "██████████ : n█████ Size = %d, ██████████ Size = %d";
    *(DWORD *)v108 = █████;
    v107 = █████;
    v106 = 100;
}
else
{
    v112 = "██████████ : Potential buffer over flow, n█████ Size";
    *(DWORD *)v108 = █████;
    v107 = █████;
    v106 = 10;
}
msg(188, v106, v107, *(int *)v108, v112, cb);
v37 = █████MemAlloc(2 * cb);
```



# Input validation: Buffer overflow

- SpiderControl SCADA Web Server, stack-based bof,  
CVE-2015-1001

```
else
{
    strcpy((char *)&request->cookie, p + 8, line_length - 10);
    *((_BYTE *)&request->Field_48 + line_length + 2) = 0;
}
```

Se ha encontrado un problema y windows ha sido apagado para evitar daños al equipo.

El usuario final generó manualmente el volcado de bloqueo.

Si esta es la primera vez que ve esta pantalla de error de detención, reinicie su equipo. Si esta pantalla aparece otra vez, siga los siguientes pasos:

Compruebe que cualquier hardware o software está correctamente instalado. Si es una nueva instalación, contacte con su proveedor de hardware o software para obtener actualizaciones de Windows que pueda necesitar.

Si los problemas continúan, deshabilite o elimine cualquier nuevo hardware o software instalado. Deshabilite las opciones de memoria de la BIOS como caché o vigilancia. Si necesita utilizar el modo a prueba de errores para quitar

deshabilitar componentes, reinicie su equipo, presione F8 para seleccionar Opciones de inicio avanzadas y, a continuación, seleccione modo a prueba de errores.

Información técnica:

\*\*\* STOP: 0x000000E2 (0x00000000, 0x00000000, 0x00000000, 0x00000000)

Empezando el volcado de memoria física

Descarga de memoria física completa.

Póngase en contacto con su administrador de sistema o grupo de soporte técnico para obte

# RCE?

to get firmware?

to get debug symbols?

to debug?

..PowerPC

no “operation system”



# SSA-630413: Vulnerabilities in SIPROTEC 4

## Vulnerability 1 (CVE-2016-7112)

Attackers with network access to the device's web interface (port 80/tcp) could possibly circumvent authentication and perform certain administrative operations.

CVSS v3.0 Base Score 5.3

CVSS v3.0 Vector CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

## Vulnerability 2 (CVE-2016-7113)

Specially crafted packets sent to port 80/tcp could cause the affected device to go into defect mode.

CVSS v3.0 Base Score 5.3

CVSS v3.0 Vector CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

## Vulnerability 3 (CVE-2016-7114)

Attackers with network access to the device's web interface (port 80/tcp) could possibly circumvent authentication and perform certain administrative operations. A legitimate user must be logged into the web interface for the attack to be successful.

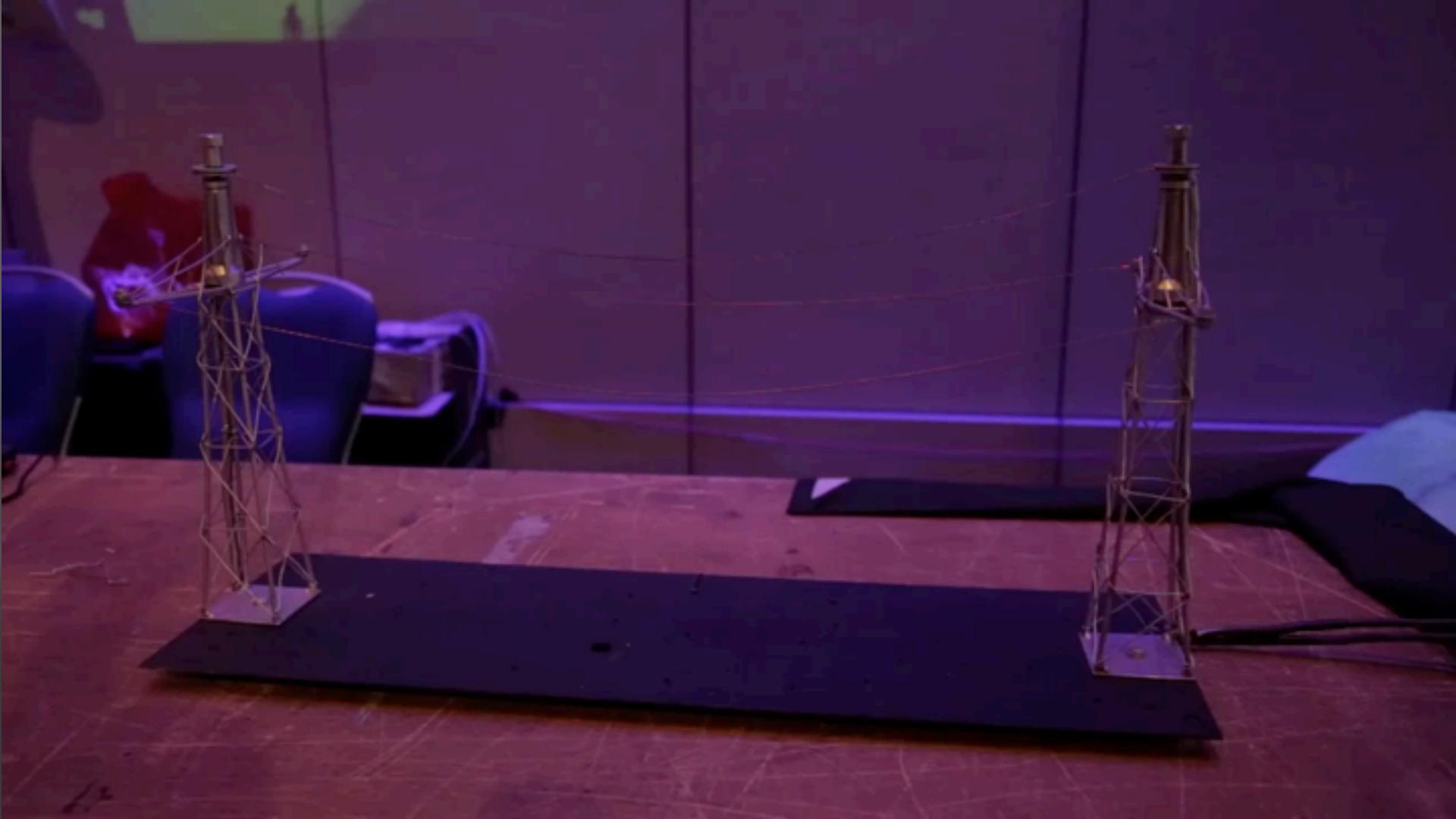
CVSS v3.0 Base Score 4.3

CVSS v3.0 Vector CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N

File Edit View Terminal Tabs Help

user@nesterovk-nb ~ 16:10:09

\$ nmap -T4 -F 192.168.0.42

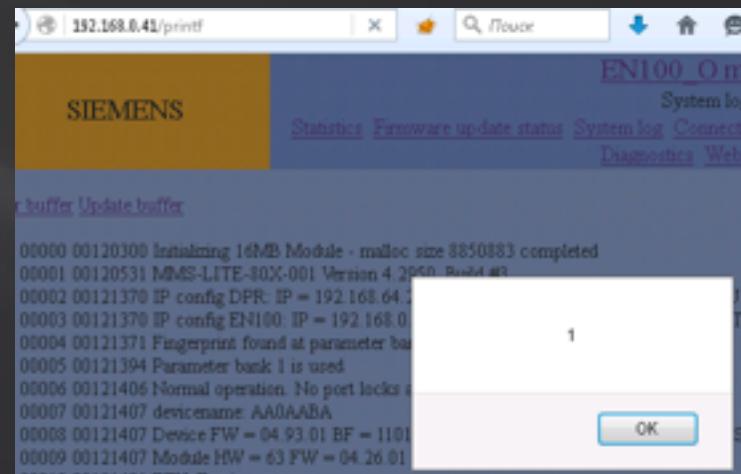


# Code vulnerabilities

- Siemens SIPROTEC 7SJ64 (protective relay) XSS

```
POST /upload HTTP/1.1
Host: 192.168.0.41
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:43.0) Gecko/20100101 Firefox/43
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: ru-RU,rurq=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://192.168.0.41/upload
Connection: keep-alive
Content-Type: multipart/form-data; boundary=-----2688683723308
Content-Length: 16640

-----2688683723308
Content-Disposition: form-data; name="userfile"; filename="<script>alert(1)</script>"  
Content-Type: application/octet-stream
```



# Code vulnerabilities

- Siemens WinCC

## [SSA-223158: Multiple Vulnerabilities in WinCC 7.0 SP3](#)

Publishing Date	2012-06-05
Last Update	2012-06-05
Current Version	V1.0
CVSS Overall Score	5.3

### Summary:

Several vulnerabilities in the web server and the web application of WinCC 7.0 SP3 were discovered recently. These vulnerabilities include:

- X-Path Injection in two web applications
- Directory Traversal in two web applications
- Buffer overflow allowing a denial-of-service attack in WinCC DiagAgent web server
- Reflected Cross-Site Scripting in two web applications
- Open redirect in one web application

There are several mitigating factors (see below for details).

All of these weaknesses except the buffer overflow are closed with the Update 2 for WinCC V7.0 SP3. The buffer overflow was not fixed, because the vulnerable DiagAgent is turned off by default and will not be distributed or supported anymore. See below for alternatives.

### AFFECTED PRODUCTS

- WinCC 7.0 SP3

# Story of CVE-2013-3957

## National Cyber Awareness System

### Vulnerability Summary for CVE-2013-3957

**Original release date:** 06/14/2013

**Last revised:** 06/17/2013

**Source:** US-CERT/NIST

## Overview

SQL injection vulnerability in the login screen in the Web Navigator in Siemens WinCC before 7.2 Update 1, as used in SIMATIC PCS7 8.0 SP1 and earlier and other products, allows remote attackers to execute arbitrary SQL commands via unspecified vectors.

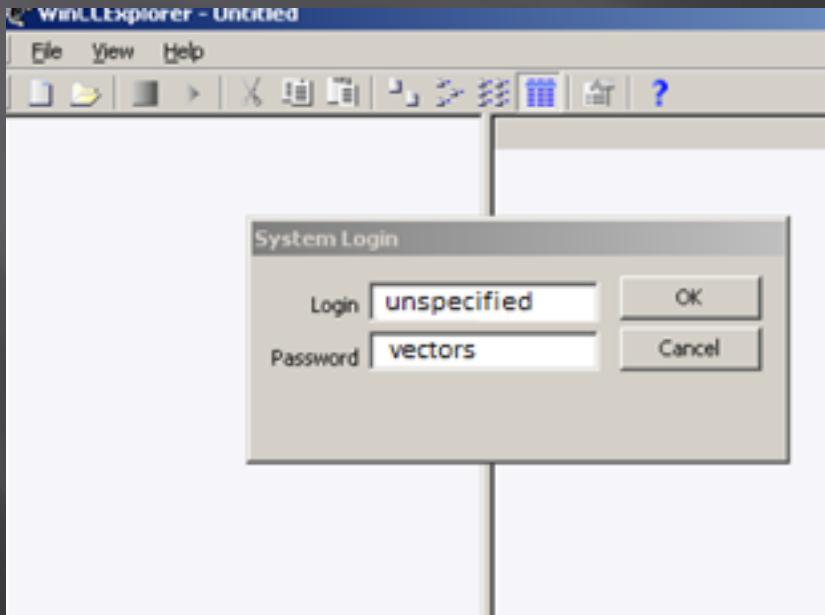
# Cisco for the rescue!

The screenshot shows a Cisco website page for security intelligence operations. The top navigation bar includes links for Products & Services, Support, How to Buy, Training & Events, and Partners. A search bar is also present. The main content area displays a threat bulletin titled "Cisco Applied Mitigation Bulletin: Identifying and Mitigating the Siemens WinCC Web Navigator Vulnerabilities". The bulletin details threat type (CWE-264), Intellishield ID (29768), version (1), and publication dates. It also includes severity levels (Unlikely Use, Confirmed, Mild Damage) and a summary of the vulnerability. On the right side, there's a sidebar for "Related Links" including Solutions, Security Solutions, E-mail Security, and Threat Control for Endpoints. The main content area contains configuration code for access lists:

```
!-- The following vulnerability-specific access control entries
!-- (ACEs) can aid in identification of attacks against these vulnerabilities
!
access-list 150 deny tcp any 192.168.60.0 0.0.0.255 eq 80
access-list 150 deny tcp any 192.168.60.0 0.0.0.255 eq 443
```

!-- The following vulnerability-specific access control entries  
!-- (ACEs) can aid in identification of attacks against these vulnerabilities  
!  
access-list 150 deny tcp any 192.168.60.0 0.0.0.255 eq 80  
access-list 150 deny tcp any 192.168.60.0 0.0.0.255 eq 443

# WinCC SCADA-Clients?



WinCCEexplorer.exe/PdlRt.exe

Create and use your own security features  
Instead of standard features – that's  
A bad idea!

# Hardcoded secrets

- Hardcodes are for protocols with auth: SNMP, telnet, HTTP, etc.
- You can hardcode keys, certificates, passwords
- SMA Sunny WebBox

```
// Decompiled with JetBrains decompiler
// Type: nSecurity.AccessLevels
// Assembly: WebBox, Version=1.53.12.70, Culture=neutral, PublicKeyToken=null
// MVID: 9F73EB29-EA97-48B2-9E93-8BAC4830E834
// Assembly location: C:\update\run\WebBox.exe

namespace nSecurity
{
    public enum AccessLevels : byte
    {
        NONE,
        LOCKED,
        USER,
        INSTALLER,
        SERVICE,
        DEVELOPER,
    }
}
```

```
// Type: SMA.Update.Packager.PasswordMode
// Assembly: SMA.Update.Packager, Version=1.1.6.3, Culture=neutral, PublicKeyToken=null
// MVID: 23DAEB8A-63BB-4877-8B4C-3D6ADD950CBA
// Assembly location: C:\update\run\sma.update.packager.dll

namespace SMA.Update.Packager
{
    internal enum PasswordMode
    {
        HardCodedPw,
        AskUser,
        ActPw,
        ConfigPW,
    }
}
```

# Hardcoded secrets

- Siemens SIPROTEC 4 protective relay confirmation code

“311299”:

- System log
- Device info
- Stack and other parts of memory
- More ?

```
- send packets:  
17 bytes (0x11)  
00000000 00 00 00 00 00 01 0d 01 00 01 00 00 a1 00 00 00 .....  
00000010 00  
  
00000000 00 00 00 00 00 02 0d 01 00 01 00 00 14 01 01 08 .....  
00000010 9c 9b 06 24 c8 32 60 72 0b 18 3e 50 71 74 67 4e ...$..2'r..>PqtgN  
fHac RPN  
00000020 66 48 61 63 20 20 20 20 20 20 52 50 4e 20 20 O. .Kom C.eana  
00000030 20 4f 97 20 20 00 4b 6f 6d 20 43 81 65 61 6e 61 =ACS Mfrs .....  
00000040 3d 41 63 73 20 4d 66 72 73 20 00 00 14 a0 00 13  
00000050 b6 be 06 24 c8 f3 60 72 0b 18 4e 66 69 72 70 71 ...$. 'r..Nfirpq  
00000060 20 6b 61 6e 61 6c 20 31 20 20 20 52 50 4e 20 20 kanal 1 RPN  
00000070 20 4f 97 20 20 20 4b 6f 6d 20 43 81 65 61 6e 61 O. Kom C.eana  
00000080 3d 41 63 73 20 4d 66 72 73 20 00 a0 00 08 a1 a2 =ACS Mfrs .....  
00000090 00 03 06 24 c8 f3 60 72 0b 18 4e 66 69 72 70 71 ...$. 'r..Nfirpq  
000000a0 20 6b 61 6e 61 6c 20 32 20 20 20 52 50 4e 20 20 kanal 2 RPN  
000000b0 20 4f 97 20 20 20 4b 6f 6d 20 43 81 65 61 6e 61 O. Kom C.eana  
000000c0 3d 41 63 73 20 4d 66 72 73 20 00 a5 ae a5 a5 a5 =ACS Mfrs .....  
000000d0 a7 00 06 24 c9 ed 60 72 0b 18 4b 6e 53 78 58 61 ...$. 'r..KnsXxa  
000000e0 72 81 51 61 62 6f 73 81 3e 20 20 52 50 4e 20 20 r.Qabos.> RPN  
000000f0 20 4f 97 20 20 20 4b 6f 6d 20 43 81 65 61 6e 61 O. Kom C.eana  
00000100 3d 41 63 73 20 4d 66 72 73 20 00 22 22 02 a5 a5 =ACS Mfrs .""..  
00000110 a7 00 06 24 ca 28 60 72 0b 18 54 72 73 71 6f 6a ...$.('r..Trsqoj  
00000120 72 73 63 6f 20 4f 4b 20 20 20 52 50 4e 20 20 rsco OK RPN  
00000130 20 4f 97 20 20 20 4b 6f 6d 20 43 81 65 61 6e 61 O. Kom C.eana  
00000140 3d 41 63 73 20 4d 66 72 73 20 00 20 49 6e 66 6f =ACS Mfrs . Info  
00000150 5f 30 06 24 cb 09 60 72 0b 18 44 69 62 30 31 20 _0.$..r..Dib01  
00000160 41 6b 73 69 63 6e 61 20 20 20 52 50 4e 20 20 Aksicna RPN  
00000170 20 4f 97 20 20 20 4b 6f 6d 20 43 81 65 61 6e 61 O. Kom C.eana
```

# Hardcode secrets

- Siemens SIPROTEC 4 protective relay confirmation code “311299”:  
*“SIPROTEC 4 and SIPROTEC Compact devices allow the display of extended internal statistics and test information...”*

*To access this information, the confirmation code “311299” needs to be provided when prompted.”*

*“...Siemens **does not publish official documentation** on these statistics. It is strongly recommended to work together with Siemens SIPROTEC customer care or commissioning experts to retrieve and interpret the statistics and test information...”*

# Please change IP address to <whatever>

- Siemens S7-1200 PLC, CVE-2014-2252

*“An attacker could cause the device to go into defect mode if specially crafted PROFINET packets are sent to the device. A cold restart is required to recover the system.”*

Just “set” PROFINET request: set network info (ip, netmask, gateway) with all zero values.

# Kiosk mode restrictions bypass

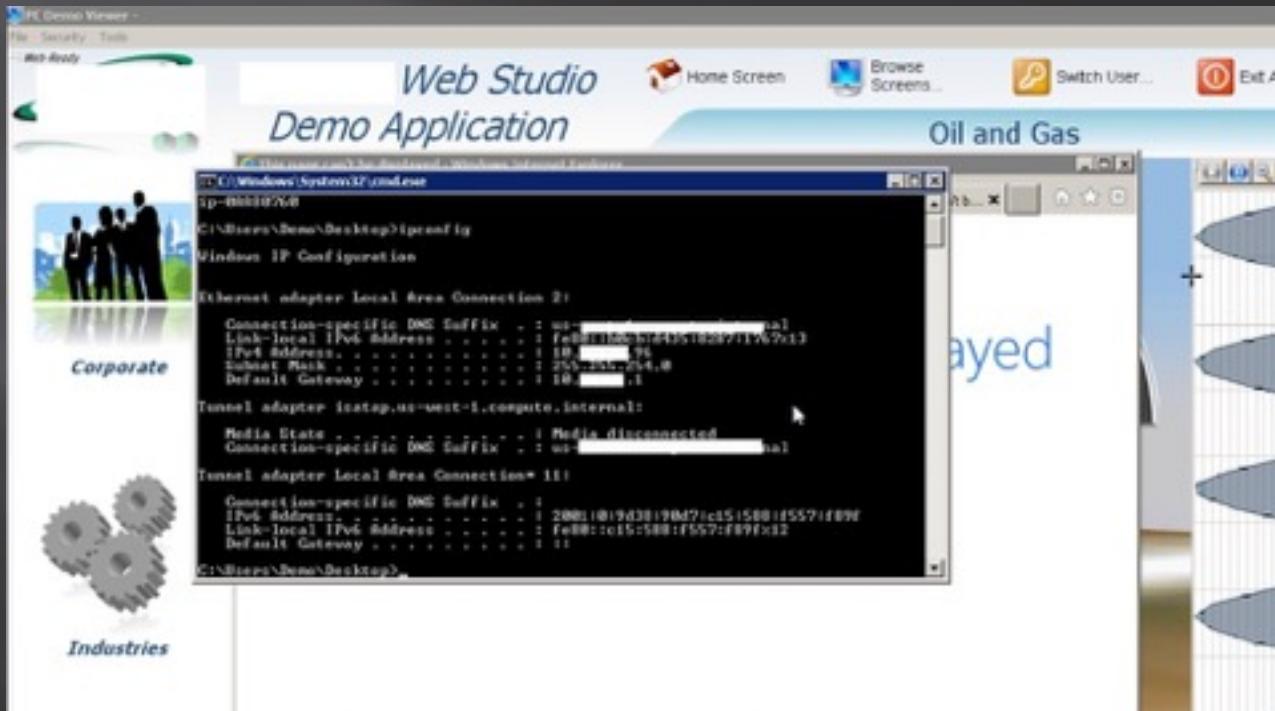
KIOSK mode:

Limit access to OS functions



# Kiosk mode restrictions bypass

KIOSK mode: Limit access to OS functions



# Cryptofails: hardcoded key for XOR, lol

- Wincc accounts: “secret” crypto key

```
strEncryptionkey = "This is my encryptionkey";
for( k = 0; k < 24; ++k )
{
    result = (char *)(unsigned __int8)cutLogin[k];
    if ( cutLogin[k] || cutPass[k] )
    {
        strEncrString[k] = cutPass[k] ^ cutLogin[k];
        result = (char *)(strEncryptionkey[k] ^ (unsigned __int8)strEncrString[k]);
        strEncrString[k] = (char)result;
    }
}
```

key = "This is my encryptionkey";

# Cryptofails: hardcoded key for XOR, lol

- WinCC accounts: “secret” crypto key fixed
- It’s XOR, they should not bother hardcoding for XOR

The image shows a debugger interface with assembly code and memory dump panes. Red arrows point from the assembly code to specific memory locations in the dump pane.

```
strEncryptionkey = "This is my encryptionkey";
for ( k = 0; i < 24; ++k )
{
    wstrKey[i] = strEncryptionkey[i];
}
```

Annotations:

- A red box highlights the string `"This is my encryptionkey";` in the assembly code.
- A red box highlights the variable `wstrKey` in the assembly code.
- A red box highlights the value `+1337` in the assembly code.
- A red box highlights the string `L"This13s@My**+encryptronkeyu"` in the memory dump pane.
- A red box highlights the value `0x30u` in the memory dump pane.

Memory Dump (wstrKey):

(wstrKey, L"This13s@My**+encryptronkeyu", 0x30u);
---

# Cryptofails: Elusive OR

PLC password “encryption”

13542 800.250349000 10.0.72.31 176.12.128.189 57COMM 23338 > 102 PDU-Type:[Userda... X

- TPKT, Version: 3, Length: 37
- ISO 8073 COTP Connection-Oriented Transport Protocol
- S7 Communication
- Header: (Userdata)
  - PDU Type: Userdata (7)
    - Reserved: 0x0000
    - Sequence number: 1
    - Parameter length: 8
    - Data length: 12
  - Parameter: (Request ) ->(Security) ->(PLC password)
    - Parameter head: 0x000112
    - Parameter length: 4
    - Unknown (Request/Response): 0x11
    - 0100 .... = Type: Request (4)
    - .... 0101 = Function group: Security (5)
    - Subfunction: PLC password (1)
    - Sequence number: 0
- Data
  - Return value: Item OK (0xff)
  - Transport size: OCTET STRING (0x09)
  - Length: 8
- [Dissector bug, protocol s7COMM: proto.c:1847: failed assertion "hfinfo->hf[0].name != NULL"]
- [Expert Info (Error/Malformed): proto.c:1847: failed assertion "hfinfo->hf[0].name != NULL"]

0000	00 1c 7f 33 25 33 4c 72	b9 25 39 88 08 00 45 00	...3%3LP .%9...E.
0010	00 4d 07 37 40 00 80 06	00 00 00 0a 00 48 af b0 0c	.M.70... ....H...
0020	80 bd 5b 2a 00 66 af d4	ec 69 00 4e 41 e2 50 18	...[*.f... 1.NG.P.
0030	fa bf 83 28 00 00 03 00	00 25 02 f0 80 32 07 00	...(..... .%.2..
0040	00 00 01 00 08 00 0c 00	01 12 04 14 45 01 00 ff	.....E...
0050	09 00 08 64 64 00 00 64	64 11 11	....dd..d d..

```
s[0] = pwd[0] ^ 0x55
s[1] = pwd[1] ^ 0x55
for (int i=2; i<8; i++)
    s[i] = pwd[i] ^ s[i-2] ^ 0x55
```

Password (8 bytes)

# Cryptofails: weak algorithms

- TIA Portal PEData.plf passwords history

00120540	00 00 00 18 00 00 00 01 00 00 00 03 00 00 00 5D	.....]
00120550	00 00 00 64 00 00 00 0E 00 00 00 00 00 00 00 00	..d.....
00120560	00 00 00 00 00 00 00 00 2D 00 14 00 00 00 00 00	.....-
00120570	00 00 00 00 00 00 00 00 01 00 00 00 01 01 00 00	.....
00120580	00 00 00 00 BD 00 19 63 08 5F C3 51 65 32 9E A1 F8	.3A... c. TQe7n9n N-ZMeM
00120590	0C 5E CB DB BE E5	.....
001205A0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
001205B0	00 00 00 00 00 00 00 00 00 07 C2 80 C2 80 C2 80 07	.....BBBBBB
001205C0	C2 80 C2 80 C2 80 00 00 00 00 00 00 00 00 00 00 00 00	BBBBBB.....
001205D0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
001205E0	00 00 00 00 00 00 00 00 00 00 74 00 06 00 18 20 02	.....z.....
001205F0	00 1C 10 10 00 01 06 00 00 00 00 00 00 00 0C 20 01	.....
00120600	00 28 10 02 00 24 04 00 00 00 00 00 00 03 20 01	.{...6.....
00120610	00 1C 10 10 00 01 06 00 00 00 00 00 00 00 1A 20 02	.....

# Cryptofails: Plain and Clear

- Winccwebbridge.dll: please hash your hardcoded account

```
v28 = 1024;
if ( v11->GetServerVariable(v11, "QUERY_STRING", &Str1, (LPDWORD)&v28) && Str1 && !strcmp(&Str1, "STATUS", 6u) )
{
    if ( !strcmp(_____, puNotify->pSzUser) || !strcmp(_____, puNotify->pSzUser) )
    {
        if ( !strcmp(_____, puNotify->pSzPassword) )
        {
            v12 = *v31;
            v28 = 1024;
            if ( v12->GetServerVariable(v12, "URL", &Str1, (LPDWORD)&v28) )
            {
                if ( !strcmp(&Str1, "/bin/WinCCWebBridge.dll") )
                    goto LABEL_6;
            }
        }
    }
}
```

# Cryptofails: weak PRNG

- Siemens S7-1200, S7-1500 PLC, CVE-2014-2250,  
CVE-2014-2251

## INSUFFICIENT ENTROPY<sup>j</sup>

Because of low entropy in its random number generator, the authentication of the integrated web server (Port 80/TCP and Port 443/TCP) of S7-1500 PLCs might allow attackers to hijack web sessions over the network without authentication.

CVE-2014-2251<sup>k</sup> has been assigned to this vulnerability. A CVSS v2 base score of 8.3 has been assigned; the CVSS vector string is (AV:N/AC:M/Au:N/C:P/I:P/A:C).<sup>l</sup>

## INSUFFICIENT ENTROPY<sup>g</sup>

Because of low entropy in its random number generator, the integrated web server's authentication method (Port 80/TCP and Port 443/TCP) could allow attackers to hijack web sessions over the network if the session token can be predicted.

CVE-2014-2250<sup>h</sup> has been assigned to this vulnerability. A CVSS v2 base score of 8.3 has been assigned; the CVSS vector string is (AV:N/AC:M/Au:N/C:P/I:P/A:C).<sup>i</sup>

# Cryptofails: weak PRNG

- Siemens S7-1200, S7-1500 PLC, CVE-2014-2250, CVE-2014-2251
- Seed = plc\_start\_time + const

```
class siRand():
    def update(self):
        self.seed = (self.seed * 0x196680 + 0x3C6EF35F) & 0xFFFFFFFF
        return self.seed

    def __init__(self, seed):
        self.seed = seed
        for i in xrange(8): self.update()
        self.state = [self.update() for i in xrange(32)]
        self.index = self.state[31] & 0x1F

    def next(self):
        state = self.state[self.index]
        self.state[self.index] = self.update()
        self.index = state & 0x1F
        return state & 0xFFFFFFFF

def genSecret(seed, skip = 0):
    rng = siRand(seed)
    for i in xrange(skip): rng.next()
    return ''.join(struct.pack(">H", rng.next() & 0xFFFF) for i in xrange(8))
```

# Story of PLC ownage

Target – Siemens S7-1200 PLC



# Story of PLC ownage

PmzR9733Q8rG3LpjCGZT9N/ocMAAQABAACK1woAqsgAAAAAAAAAAIrXIUM=  
uLiHXZUTy2GMgjr1KmgmcNN/ocMAAQACAAKK1woAqsgAAAAAAAAAAIrXIUM=  
Mu/vgilgtrxq0LVp26nkMtN/ocMAAQADAAKK1woAqsgAAAAAAAAAAIrXIUM=  
tjH6vtNWCfa+QZHPDtCnKdN/ocMAAgADAACK1woAqsgAAAAAAAAAAIrXIUM=

3e6cd1f7bdf743cac6dcba708c21994fd37fa1c30001000100028ad70a00aac80000000000000008ad72143  
b8b8875d9513cb618c823af52a682670d37fa1c30001000200028ad70a00aac80000000000000008ad72143  
32efef822220b6bc6ad0b569dba9e432d37fa1c30001000300028ad70a00aac80000000000000008ad72143  
b631fabed35609f6be4191cf0ed0a729d37fa1c30002000300028ad70a00aac80000000000000008ad72143

# Story of PLC ownage

3e6cd1f7bdf743cac6dcba708c21994f	MD5 of ? (16bytes)
d37fa1c3	CONST (4 bytes)
0001	user logout counter (2 bytes)
0001	counter of issued cookies for this user (2 bytes)
00028ad7	value that doesn't matter (4 bytes)
0a00aac8	user IP address (10.0.170.200) (4 bytes)
00000000000000008ad72143	value that doesn't matter (12 bytes)

What about **3e6cd1f7bdf743cac6dcba708c21994f** ?

# Story of PLC ownage

MD5( NEXT 26 BYTES OF COOKIE + 16BYTES OF SECRET + 2 NULL BYTES)

What is SECRET ?

SECRET generates after PLC start by ~PRNG.

PRNG is a little bit harder than standard C PRNG.

SEED in {0x0000 ,0xFFFF}

# Story of PLC ownage

SEED very often depends on time value

SEED = PLC START TIME + 320

320 by practical way: secret generates after ~ 3-4 seconds of PLC start using current time

PLC START TIME = CURRENT TIME – UPTIME

Current time via web interface

Uptime via SNMP with hardcoded  
read community string “public”

# Story of PLC ownage

Profinet “feature” and PRNG vulnerability - real attack vector. Result - PLC takeover.



010100101

010100101

root@pc: ~

```
root@pc:~# recordmydesktop
Initial recording window is set to:
X:0 Y:0 Width:1366 Height:768
Adjusted recording window is set to:
X:6 Y:0 Width:1354 Height:768
Your window manager appears to be Metacity
```

```
Initializing...
Buffer size adjusted to 4096 from 4096 frames.
Opened PCM device hw:0,0
Playback frequency 22050Hz is not available...
Using 44100Hz instead.
Recording on device hw:0,0 is set to:
2 channels at 44100Hz
Capturing!
```

(8) 0:bash 1:bash\* 2:recordmydesktop\*

"pc" 08:03 08-Oct-14

010100101

# Cryptofails: Your hand in mine

- Hash passwords
  - SHA is not good enough
  - Put length of plaintext nearby

Redbox\_value = len(pwd)\*2+1

00120540	00 00 00 18 00 00 00 01 00 00 00 03 00 00 00 5D	.....]
00120550	00 00 00 64 00 00 00 0E 00 00 00 00 00 00 00 00	..d.....
00120560	00 00 00 00 00 00 00 00 00 2D 00 14 00 00 00 00	.....-
00120570	00 00 00 00 00 00 00 00 00 01 00 00 00 01 01 00	.....
00120580	00 00 40 BD 00 15 63 08 5F C3 51 65 32 9E A1 FF	..BS...c. TQz2hYw \\JNhs[.....
00120590	5C SE CB DB BE EF 00 00 00 00 00 00 00 00 00 00 00	.....
001205A0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
001205B0	00 00 00 00 00 00 00 00 00 07 C2 80 C2 80 C2 80 07	.....BBBBBB.....
001205C0	C2 80 C2 80 C2 80 00 00 00 00 00 00 00 00 00 00 00 00	BBBBBB.....
001205D0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
001205E0	00 00 00 00 00 00 00 00 00 74 00 06 00 18 20 02	.....E.....
001205F0	00 1C 10 10 00 01 06 00 00 00 00 00 00 0C 20 01	.....
00120600	00 28 10 02 00 24 04 00 00 00 00 00 00 03 20 01	.(....S.....
00120610	00 1C 10 10 00 01 06 00 00 00 00 00 00 1A 20 02	.....

# Industrial protocols

“Secure” set up speed of energetic turbine

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00000000	FA	CE	00	80	00	02	58	1F	00	01	1D	B2	54	80	01	00
00000010	0A	01	00	00	6A	A0	00	10	13	12	01	2C	00	08	00	00
00000020	00	0A	00	04	00	0A	00	14	00	1A	00	1C	00	02	00	25
00000030	00	02	00	27	00	04	00	29	00	0A	00	2A	00	06	00	48
00000040	00	00	00	00	00	9B	13	32	00	06	00	41	00	4F	00	31
00000050	00	2F	00	53	00	50	00	00	00	02	00	43	00	56	00	00
00000060	47	00	02	00	35	00	37	00	00	00	00	00	01	00	0D	G...5.7.....
00000070	00	41	00	44	00	4D	00	49	00	4E	00	49	00	53	00	54
00000080	00	52	00	41	00	54	00	4F	00	52	00	00	6A	A0	00	01
00000090	B3	C1														iB

More details at “SCADA deep inside: protocols and security mechanisms”

# Industrial protocols

# Industrial protocols: S7-300 PLC password cracker.

Included in the popular tool `thc-hydra`.

root@pt:~/3OC3#

```

0000  20 cf 30 50 c3 85 54 7f ee d0 ff 7c 08 00 45 00  .0P..T
....|.E.
0010  00 28 98 2e 40 00 7f 06 5e b8 0a 00 aa bf 0a 00  .(./8..
|^.....|
0020  46 2a 00 66 b2 53 1c 25 9b 10 9b 50 a3 7a 50 14  F*.E.S.
4...P..S.
0030  00 00 01 4d 00 00 00 00 00 00 00 00 00 00 00 00  ...H...
|||||_
3262.108376 10.0.170.191 -> 10.0.30.42    TCP 60 iso-tsap > 4565
2 [RST, ACK] Seq=1 Ack=23 Win=0 Len=0

0000  20 cf 30 50 c3 85 54 7f ee d0 ff 7c 08 00 45 00  .0P..T
....|.E.
0010  00 28 98 2f 40 00 7f 06 5e b7 0a 00 aa bf 0a 00  .(./8..
|^.....|
0020  46 2a 00 66 b2 54 38 95 72 9c a5 43 5d b7 50 14  F*.E.TB
4...C..P.
0030  00 00 4a 00 00 00 00 00 00 00 00 00 00 00 00 00  ...J....
|||||_

```

Hi 30C3 : Im gonna show you how to find, identify and brute password for Siemens S7-300 PLC

卷之三

-- INSERT --

"pt" 02:45 26-Dec-13

# harrassment

```
        alert(Html2xml(oNode));
        oxml.LoadXML("<NODES>" + oNode.innerHTML + "</NODES>");
        alert(oxml.xml);
        return oxml.transformNode(strPattern);
    }

    // dreckige Hackerei
    function Html2xml(oNode)
    {
        // copy the attributes first
        var attb;
        var str = new String;
        str = "<" + oNode.tagName;
        for(attb in oNode.attributes)
        {
            var attbval = oNode.getAttribute(attb);
            if(attbval != null && attbval != "")
            {
                str += " " + attb.nodeName + "=" + oNode.nodevalue + " ";
            }
        }
    }
}
```

```
// dreckige Hackerei
function Html2xml(oNode)
{
    // copy the attributes first
    var attb;
```

# FyN

Daily Overview  
1/10/15 11:50:00 am

All ROOF TOP ROW ROOF BOTTOM ROW AWNING BARN ROOF - RADIAN

10 kW  
8 kW  
6 kW  
4 kW  
2 kW

10:00 am

PT-2015-01: SQL Injection in Solar-Log WEB

Severity: High (7.5) (AV:N/AC:L/Au:N/C:P/I:/P/A:P)  
Fix date: 13.01.2015  
Vector: Remote  
Systems affected: Solar-Log WEB  
Vendor: Solare Datensysteme GmbH  
Notification status: 12.01.2015 - Vendor gets vulnerability details  
13.01.2015 - Vendor releases fixed version and details  
13.02.2015 - Public disclosure

Current

Feed-in Power Pdc  
Generator Power Pdc  
Inverter Efficiency %  
Status  
Error

3x Mpp, Power

Maximum Value	Target	Actual Value
1.97 kW	6.05 kWh	53.78 %

# FyN

Don't patch too much

ICS-CERT sent by matthew.kress-weitenhagen@inl.gov

Sent: Friday 11 April 2014 18:29

To: Sergey Gordeychik

Cc: ics-cert-soc@hq.dhs.gov; CSOC; Gleb Gritsai

 You replied to this message on 11/04/14 21:03.

Mr. Gordeychik,

From my initial analysis, this product does not appear to be sold in the United States. We will continue to look into this but I would

# FyN

Wait a second....

## New Solar-Log® & GE Meter Ready for the US Solar Market

An easy to install, all-inclusive, cost effective device for residential installations.



The new Solar-Log(R) & GE Meter

The new Solar-Log(R) & GE Meter

# Projects

- We work with responsible disclosure approach
- Full disclosure = all vuln details immediately in the wild. Giving the vendors absolutely no opportunity to release a fix
- Responsible disclosure = researcher contacts the vendor before the vulnerability is released. And all stakeholders agree to allow a period of time for the vulnerability to be patched before publishing the details.
- Because vulnerability patching very important for ICS and can take months. Even years.

# Projects

- > That's why responsible disclosure in ICS highly important

**Google just disclosed a major Windows bug — and Microsoft isn't happy**

*Is 10 days enough time to build a patch?*

by Russell Brandom | @russellbrandom | Oct 31, 2016, 4:57pm EDT

[SHARE](#) [TWEET](#) [LINKS](#)



Today, Google's Threat Analysis group [disclosed a critical vulnerability in Windows](#), in a public post on the company's security blog. The bug itself is very specific — allowing attackers to escape from security sandboxes through a flaw in the win32k system — but it's serious enough to be categorized as critical, and according to Google, it's being actively exploited. As

**NOW TRENDING**



The best Black Friday TV deals from Walmart, Best Buy, Amazon, and more



Tesla powers a whole island with solar to show off its energy chops

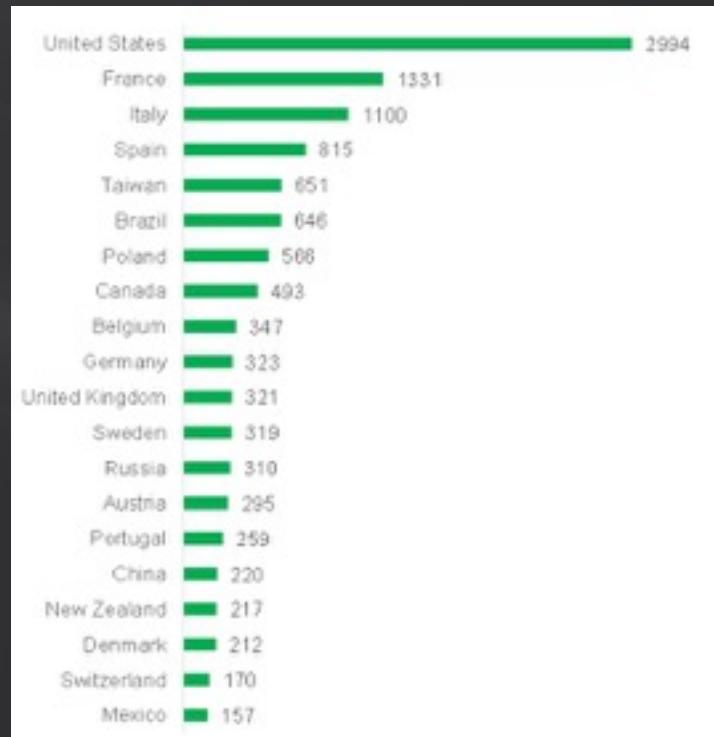
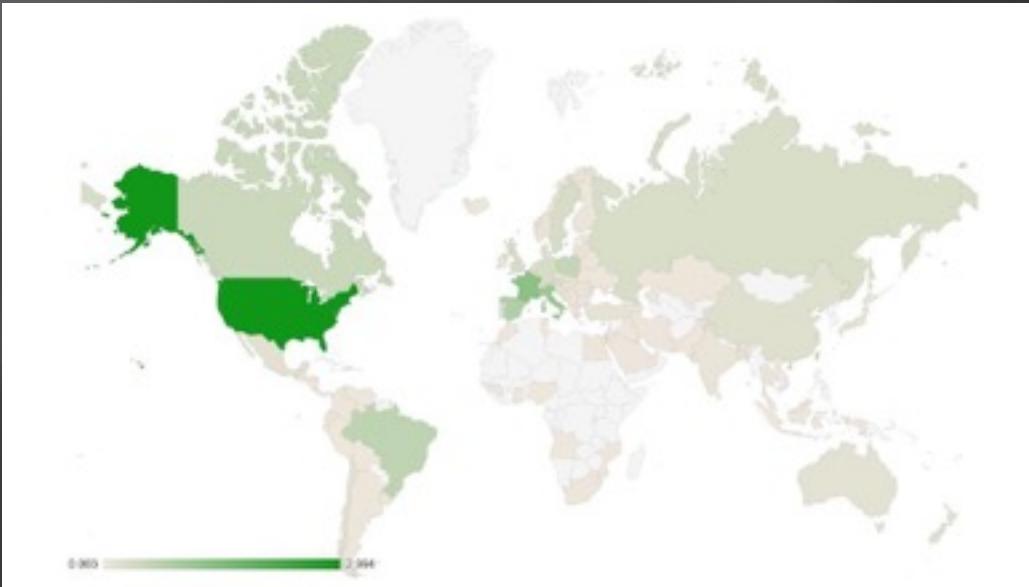
# Projects

1. Research
2. We send details directly to vendor and CERT
3. Vendor create CVE
4. Vulnerability patched
5. SCADASL public disclosure and exploit/toolkit publishing
6. Applause to SCADASL
7. Research
8. ...

# Projects

Analytics every year:

- ICSMAP
- ICSDORKS



# Projects

## ➤ #SCADAPASS

- Release 1.2
- 37 vendors
- PLC, RTU, gateways, switches, servers ...

# Projects

## > #SCADASOS

(un)Secure Open SmartGrids is open initiative to rise awareness on insecurities of SmartGrid, Photovoltaic Power Stations and Wind Farms

# Projects

Q: How to participate

A: Find Internet-connected PV and Wind power stations and notify vendors/CERTs/community.

Q: Wow! It simple! Can I hack it?

A: No. It can be a hospital or your grandma's cottage. Please use passive approach (firmware analysis, testbeds etc.)

Q: I get an 0day!

A: Please submit it to vendor and/or regional CERT

Q: What will I get?

A: Kudos at SCADA StrangeLove Talks/Knowledge/Safer World.

Details

You can make shodan saved search or drop google dorks to twitter

Please use tags #solar #wind #scadasos

# Projects

- 60 000+ SmartGrid devices disconnected from the Internet
- Two Advisories
  - XZERES 442SR Wind Turbine CSRF
  - SMA Solar Technology AG Sunny WebBox Hard-Coded Account Vulnerability

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

SMA Solar Technology AG Sunny WebBox Hard-Coded Account Vulnerability (Update A)

Original release date: September 03, 2015 | Last revised: September 17, 2015

[Go Home](#) [Tweet](#) [Send](#) [Share](#)

**Legal Notice**

All information products included in <http://www.us-cert.gov> are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see <http://www.us-cert.gov/tlp>.

---

**OVERVIEW**

This updated advisory is a follow-up to the advisory titled ICSA-15-181-02 SMA Solar Technology AG Sunny WebBox Hard-Coded Account Vulnerability that was published September 3, 2015, on the NCCIC/ICS-CERT web site.

Aleksandr Timonin of PT Security has identified a hard-coded account vulnerability in SMA Solar Technology AG's Sunny WebBox product. SMA is planning to discontinue the sale of this product, and there is no plan to fix old versions. They have reached out to WebBox users with compensating security recommendations.

This vulnerability could be exploited remotely.

**Advisory (ICSA-15-155-01)**

XZERES 442SR Wind Turbine CSRF Vulnerability

Original release date: June 04, 2015

[Go Home](#) [Tweet](#) [Send](#) [Share](#)

**Legal Notice**

All information products included in <http://www.us-cert.gov> are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see <http://www.us-cert.gov/tlp>.

---

**OVERVIEW**

Independent researcher Maxim Rupp has identified a cross-site request forgery (CSRF) vulnerability in XZERES's 442SR turbine generator operating system (OS). XZERES has produced a patch to mitigate this vulnerability. This vulnerability could be exploited remotely.

**AFFECTED PRODUCTS**

The following XZERES product is affected:

- 442SR Wind Turbine

# Projects

Current and future:

- Smart energy generation
- Rail road and signaling systems
- Digital substations
- GSM/GPRS modems

# Results

- Well-known and habitual world of information security growing up, evolving, changing quickly
- Because a lot of specialists involved in it
- Unfortunately ICS security area not very mobile and changeable
- Also our team members growing old, starting a families
- We think that our mission done successfully



# Results

- But not finished yet....



# Results

Still trying to hack ICS, son?

Have you ever heard  
about  
SCADASTRANGELOVE ?!



# Results

- All materials at SCADA.SL
- We hope that our work can help you create your own projects.  
But don't forget about community and responsible disclosure principle





\*All pictures are taken from  
Google and other Internets

# THANK YOU

Alexander Timorin  
Alexander Tlyapov  
Alexander Zaitsev  
Alexey Osipov  
Andrey Medov  
Artem Chaykin  
Denis Baranov  
Dmitry Efanov  
Dmitry Nagibin  
Dmitry Serebryannikov  
Dmitry Sklyarov  
Evgeny Ermakov  
Gleb Gritsai  
Ilya Karpov  
Ivan Poliyanchuk  
Kirill Nesterov  
Roman Ilin  
Sergey Bobrov  
Sergey Drozdov  
Sergey Gordeychik  
Sergey Scherbel  
Timur Yunusov  
Valentin Shilnenkov  
Vladimir Kochetkov  
Vyacheslav Egoshin  
Yuri Goltsev  
Yuriy Dyachenko